$ cat 1984

2600: THE HACKER DIGEST - VOLUME 1

$

COVERS

1984 was the first year of our newsletter phase, which lasted through 1986. So we didn't really have covers in the traditional sense. We did, however, try to have as much fun as we could with our masthead. Here you can trace the evolution as we started to experiment with new things.

As evidenced in the really tiny print, we originally had expected to be a nonprofit organization. That wound up being a whole lot more involved than we wanted to get and the wording was dropped in future years.

In April, we actually thought of selling back issues for the first time, and that option, along with a half-year subscription, was added. In August, we started to get international interest, and so an overseas rate was added to the masthead. We also started to use our full nine-digit zip code with enthusiasm, and added our MCI Mail address along with a Telex number that came with our Western Union Easylink account. (We never received a single Telex and we stopped listing it in December.) It wasn't until October that we finally opened an office and got a phone number. In November, we were assigned an ISSN number and began to think that maybe we'd stick with this publishing thing for a while.

Our very first issue began with an exclamation point after the date, to emphasize our spirit of defiance and surprise that we actually made it to publication. (A federal hacking investigation in 1983 had almost derailed the entire thing.) And, of course, it was fun to finally see the year 1984 arrive. The exclamation point for the first issue of the year would become a tradition. (Interestingly, our first story also had an exclamation point in its one word title.)

The overall look of the masthead was fairly traditional, with the name *2600* off to the left in Times Bold, a generic month and year to the right, and the volume and number in all caps and italics below that. This left a little space in the middle for us to play with, something which quickly grew out of control. It started with a simple reference to the bottom row of an expanded touch tone phone ("*0#D"), the "D" only being found on military phones and "silver boxes." This was how we filled the space for the first two issues. After that, "FSLN 3" was a reference to the Sandinista revolutionary party of Nicaragua, as well as the album "Sandinista" by The Clash, which had an "FSLN 2" catalog number on the side. In April, "SYSERRO" was a pun on what looked like a computer system error and the Roman philosopher Cicero. May saw a reference to "1+800" numbers, which were the salvation of many a phone phreak at the time. Back then, not only were 800 numbers free of charge, but they didn't ever trace your number! It was the best of all worlds. In June, the upside down message of "IT'S BACK" referred to the return of the legendary OSUNY hacker BBS, which had been down for some time. In July, it was another play on words with "JRST ICE" being an instruction on the PDP-10 computer (the JRST part, anyway), with the entire thing sounding suspiciously like "justice." (Even then, we had heard of the concept.) We're sure that the "12+1=13" note in the August issue meant something significant at the time, but we can't find anyone who remembers this one. In September, we started to make use of graphics on the front page, with a clip-art guy holding a phone and leaning on our name. The little crowd of people staring at a board on the front of the October issue just might have been a reference to the 55th anniversary of the stock market crash. The November issue had a clip-art telephone with the initials AVP on it, which may have been a reference to something within IBM or possibly the government. Finally, our December issue had the upside down word "PHALSE," a clear reference to the hacker group "Phreakers, Hackers, And Laundromat Service Employees," which were the people who got together to form *2600* back in 1983. They also caused the federal authorities to investigate a possible connection between hackers and laundromats, even though the group name was only used in order to make the acronym look and sound cool.

2600 January, 1984!

Published monthly by 2600 ENTERPRISES, an eleemosynary organization. Subscription rates are $10 annually. Write to 2600, Box 752, Middle Island, NY 11953.

*0#D

VOLUME ONE, NUMBER ONE

2600 February, 1984

Published monthly by 2600 ENTERPRISES, an eleemosynary organization. Subscription rates are $10 annually. Write to 2600, Box 752, Middle Island, NY 11953.

*0#D

VOLUME ONE, NUMBER TWO

2600 March, 1984

Published monthly by 2600 ENTERPRISES, an eleemosynary organization. Subscription rates are $10 annually. Write to 2600, Box 752, Middle Island, NY 11953.

FSLN 3

VOLUME ONE, NUMBER THREE

2600 April, 1984

Published monthly by 2600 ENTERPRISES, INC., an eleemosynary organization. Subscription rates are $10 annually, $5 semiannually, and $1 per back copy. Write to 2600, Box 752, Middle Island, NY 11953.

SYSERRO

VOLUME ONE, NUMBER FOUR

2600 May, 1984

Published monthly by 2600 ENTERPRISES, INC., an eleemosynary organization. Subscription rates are $10 annually, $5 semiannually, and $1 per back copy. Write to 2600, Box 752, Middle Island, NY 11953.

1+800

VOLUME ONE, NUMBER FIVE

2600 June, 1984

Published monthly by 2600 ENTERPRISES, INC., an eleemosynary organization. Subscription rates are $10 annually, $5 semiannually, and $1 per back copy. Write to 2600, Box 752, Middle Island, NY 11953.

IT'S BACK

VOLUME ONE, NUMBER SIX

2600 July, 1984

Published monthly by 2600 ENTERPRISES, INC., an eleemosynary organization. Subscription rates are $10 annually, $5 semiannually, and $1 per back copy. Write to 2600, Box 752, Middle Island, NY 11953.

JRST ICE

VOLUME ONE, NUMBER SEVEN

2600 August, 1984

12+1=13

2600 is published monthly by 2600 ENTERPRISES, INC., an eleemosynary organization. Subscription rates: $10—1 year, $5—6 months, $1 per back issue; overseas $13.50—1 year. Write to: *2600*, Box 752, Middle Island, NY 11953-0752; MCI Mail: 26HUNDRED; TLX: 6501994928.

VOLUME ONE, NUMBER EIGHT

2600 September, 1984

2600 is published by 2600 ENTERPRISES, INC., an eleemosynary organization. Subscription rates: $10—1 year, $5—6 months, $1 per back issue; overseas $13.50—1 year. Write to *2600*, Box 752, Middle Island, NY 11953-0752; MCI Mail: 26HUNDRED; TLX: 6501994928.

VOLUME ONE, NUMBER NINE

2600 October, 1984

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization. Subscription rates: $10—1 year, $5—6 months, $1 per back issue; overseas, $13.50—1 year. Write to *2600*, Box 752, Middle Island, NY 11953-0752; MCI Mail: 26HUNDRED; TLX: 6501994928. ATT: 5167512600.

VOLUME ONE, NUMBER TEN

2600 November, 1984

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
Subscription rates: $10—1 year, $5—6 months, $1 per back issue. Overseas: $13.50—1 year.
Write to *2600*, Box 752, Middle Island, NY 11953-0752; MCI Mail: 26HUNDRED; TLX: 6501994928. ATT: 5167512600. ISSN: 0749-3851.

VOLUME ONE, NUMBER ELEVEN

2600 December, 1984

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
Subscription rates: $10—1 year, $5—6 months, $1 per back issue. Overseas: $13.50—1 year.
Write to: *2600*, Box 752, Middle Island, NY 11953-0752; MCI Mail: 26HUNDRED. ATT: 5167512600. ISSN: 0749-3851.

ƎSLAHd

VOLUME ONE, NUMBER TWELVE

AHOY!

(That's how Alexander Graham Bell used to answer his phone. For some reason, it never caught on...)

This is the very first issue of *2600*. We will, on this page, explain our motives and what the goals are which we hope to achieve with this publication.

The idea for *2600* was born early in 1983. We saw a tremendous need for some form of communication between those who truly appreciate the concept of communication: technological enthusiasts. Of course, others have different ways of describing such people—these range from words like hacker or phreaker to stronger terms such as criminal or anarchist. Our purpose is not to pass judgement. *2600* exists to provide information and ideas to individuals who live for both. **All of the items contained on these pages are provided for informational purposes only. *2600* assumes no responsibility for any uses which this information may be put to.**

Of course, a lot has changed since our first days. *War Games* came out. And then the 414 gang got caught. Suddenly everyone was talking about phreakers and hackers. And while there were some that sort of jumped into the limelight, others were a bit more cautious, in fact, some were quite upset. Sure, the publicity was fun. But what would be the cost?

Well, time has passed and the cost has been high. Phreakers and hackers have been forced into virtual isolation. Raids by the FBI have become almost commonplace. The one magazine that was geared towards phone phreaks (*TAP*) mysteriously disappeared at the height of the crisis, sparking rumours that they, too, had been raided. However, in November, the magazine resurfaced, with an explanation that a fire had destroyed part of their mailing list. (Incidentally, if your name was one of the ones that was lost, you can claim the issues you are entitled to by sending *TAP* a copy of their mailing label or a cancelled check.)

And then there was the legendary computer bulletin board known as *OSUNY*. Enthusiasts from all across the country called up this board and left messages ranging from the latest in Sprint codes to how to crash an RSTS system to what to do once you've finally gained access to Autovon. Within a week after being mentioned in *Newsweek*, *OSUNY* was disconnected. Word has it that they are still in existence somewhere, but by invitation only. A truly smart move, if that is the case.

Many hackers were keeping a low profile even before the October raids. When the FBI confiscated equipment from 15 sites across the country on the twelfth and thirteenth of the month (sponsored by a grant from the folks at GTE), many of our contacts were lost because they feared the consequences of continuing. Two organizations, the Inner Circle and PHALSE, were deeply affected by the raids. The latter group (whose initials signify Phreakers, Hackers, and Laundromat Service Employees) is still in contact with us on occasion and has promised to contribute many articles devoted to just what was really going on.

So it seems that the events of 1983 have conspired to actually *strengthen* the resolve of hackers and phreakers across the country to put out this monthly newsletter. We hope you will help us continue by subscribing, spreading the word among your friends, and of course contributing articles and information. Since we are non-profit, it really doesn't matter to us if you xerox your copy and send it to someone else—all we ask is that you let us know so that we can have a rough idea of how many people we're reaching.

2600 has several sections, some of which will appear every month, others on an irregular basis. On this, the front page, and on page two, you will always find informative full-length features on relevant subjects. Future topics include: "A Guide to Long Distance Telephone Services and Their Vulnerabilities", "DEC and Their Many Mistakes", "Phreaking in the Sixties", and "Tracing Methods Used by the Law", as well as any late-breaking items. "FLASH" appears on page 3 and provides a roundup of timely news items written from a technological enthusiast's perspective. Page 4 is used for a variety of things—interesting stories from the past, schemes and plots that just might work, and feedback from subscribers. The last two pages of *2600* are comprised of data. Just what sort of data, we cannot say. However, if it is something that you are looking for, then you will probably recognize it.

The three holes on each page serve a purpose. We suggest that you obtain a loose-leaf book so that you can neatly file every issue of *2600* you receive.

Many thanks to those of you who subscribed without even seeing an issue. A word of advice, though: don't do it again or you'll probably get ripped off! We'd also like to thank those who took advantage of our free issue offer. If interested in subscribing, the rates and address can be found at the top of this page.

Welcome to *2600*. Turn the page and become a part of our unique world.

FBI GOES AFTER ADS HACKERS

IBM must press charges before action can be taken — Feds reveal their tactics, blow source

On this page we had originally planned to run an article entitled: ESS — Orwell's Prophecy. *At the last minute, however, we received this bombshell from an anonymous contributor. It seems that a group of hackers was making use of one of IBM's ADS systems. (Audio Distribution Systems enable users with touch-tone phones to send voice messages back and forth to each other. Look for an in-depth article on them in a future issue.) Unfortunately, as is all too often the case, one of these hackers was really an FBI informant who was taking note of all of the illegitimate users (around 40 or so). Luckily for this particular group, the informant was sloppy and left many telltale clues which gave them literally months of warning. So, when the informant decided to send a message to the system operator, advising IBM to take action against the hackers and to call the FBI for more information, the hackers were ready. The system operator's account had also been penetrated by them and hence, the message was received by the hackers first! One of them actually followed the instructions in the message and called the FBI! And for some reason, the investigator there thought he was talking to an IBM executive. This is some of what he said.*

One of the individuals that supplies me with information from time to time has uncovered a lot of abuse within the ADS systems, not only here in the United States, but in England and Italy. I talk to this individual on a private bulletin board. . .

We have no ability to come in as an outside investigative or law enforcement agency and do anything about it because, first off, we don't have a complainant. We don't want to step on anybody's toes, but it's been our policy to monitor bulletin boards and the phone phreaking activity across the country and advise commercial computer systems and corporations if we do discover certain computers along with the passwords and account numbers being published on the board. We do this on a one on one basis.

The GTE Telemail Connection

That was my baby, too! As a matter of fact, that's how we came across the ADS system — through the GTE investigation. [These] people are not just interested in data communications through terminals — they will leave voice messages on an ADS. We have been slowly uncovering more and more on the ADS in the last two months.

The major phase of [the Telemail investigation] was about 20 individuals that we had located and identified and we're looking for indictments on most of them coming down in the next month or two. We're talking about a group of highly organized people that do communicate on a daily basis all the way across the country — from San Francisco and L.A. to Denver to upstate New York. So we have a core of individuals that we are still looking at that are using your system and then we have this peripheral that we are not as concerned about because they are not part of an out & out conspiracy or an organized network, per se. I know of at least 8 or 10 that are the central figures in this, the carryover from Telemail. And we keep hearing information of other people who are calling in with junk messages — there's no real substance to their messages. Now the reason I know that is that they have included one of my sources of information onto their system and so he gets messages from the other parties.

The Communist Connection

In a way we're somewhat fortunate that it's 16-year-olds or 26-year-olds as opposed to people from behind the Iron Curtain. It gives us the opportunity to see how these systems work and see if we can plug any loopholes before somebody from a not-friendly nation would try the same thing. I personally fully expect it — I'm surprised it hasn't happened in the past. It may have. We just haven't caught it. But the kids are a little bit sloppier and they're getting caught. . . I hate to sound paranoid, but we're supposed to be considering the big picture as far as is there anything sensitive in nature. For us within the bureau, sensitive in nature first off means national security and you've got corporate trade secrets and the like that you don't need being distributed.

How the FBI Wins Trust and Gets Info

The subjects have an ego problem and they love to talk to other individuals about what they are capable of doing and bragging about it. They have a tendency to trade information. Everything is negotiable with them. We have never had to barter away access to systems — we do it more on the technical information of phone networks, computer systems, and the like to where it's more of a technical information tradeoff as opposed to an access tradeoff. [An example would be the] login procedure for a PDP-11. You integrate yourself within their confidence and their circle of friends. You feed them a little bit of bait and a lot of times they'll go for it. You enter into a dialogue with them and they end up taking you for a ride.

These people are very hungry for technical avenues through which they can communicate. It used to be the personal computer bulletin boards — public messages that anybody can read. You start finding out that they leave a phone number or an address — and you start finding out who the parties are. There's thousands of these bulletin boards across the country and you narrow in on maybe twenty or so that are the more hardcore bulletin boards that are being used for exchange of illicit information. Then they move from there to an electronic mail service, namely GTE

Telemail. They caused fits within Telemail when they decided to get a little bit cocky and see if they could shut down accounts and change passwords of the administrators and things like that. From there they have moved one step further to where they are now the same individuals communicating through the ADS systems and they also set up conference calls through the Bell System, so they're not just attacking one particular system or one individual avenue of communication — they try to hit them all. It's an ego trip for all of them.

Pen Registers

We would put a pen register on the phone line of the individual (suspect) and it would record only the digits dialed on his telephone — we would not use a full blown wiretap to record his voice. We can only put a pen register on an individual's phone for like, thirty days before we have to go back to a judge and try to get an extension and we try to minimize the use of our electronic surveillance equipment so the public does not think we're the Big Brother of 1984. (laughter) It's coming. Actually, we're already there! (hearty laughter)

We have not utilized any pen registers for the specific purposes of going after abusers of the ADS systems. First off, we have to have an actual case presented to us or a complaint. It's a roundabout way of doing it, but it's the way that we, in the bureau, have to have somebody outside come to us. Otherwise we can carry on the whole investigation without IBM even being aware that we are monitoring activity within their system and we don't want to become that secret police, or anything like that. We want to be above board and work with the corporations in the community.

Just How Much Trouble Are These Hackers In?

On the federal level we can prosecute them for telephone fraud (fraud by wire) if we can determine that the ADS is an ongoing business operation and that you are being denied your just revenues by them sneaking onto your system and abusing your system. The strictest penalty is a $1000 fine and 5 years in jail for an actual conviction of fraud by wire violation. Those are always lax — a more common sentence may be for an adult maybe a year in jail, 18 months, or a fine, sometimes they get probation, or agree to pay back any fraudulent money obtained or for services rendered or whatever to the client company — it stays on his record for a year, he's on probation for a year and at the end of that, his record is wiped clean. Rarely do they get the maximum penalty. It just doesn't happen.

Do Me a Favor

Please do not disclose any geographic location because we are kind of unique in that we do not have any other source available in any other part of the country that could supply us with information like this. He may be one of 200 people, but if you identify Michigan you identify between 2 or 3 individuals and it may burn the source.

We'd like to make it clear that we don't intend to do this kind of thing very often, since rumours about certain people being informants are very common in this business. But this is no rumour. This, friends, is solid fact — we would not have printed this story if we weren't able to substantiate the claims it makes, and we had no trouble at all doing that. Our intent in making this information known was not to screw up the FBI's fun (they're really not doing all that much out of the ordinary anyway), but rather to expose a very dangerous individual who goes by the name of Cable Pair (some say his real name is John Maxfield). This person has been posing as an extremely friendly hacker who lives in Detroit and is just bubbling over with technical information in exchange for your secrets. He claims to have been one of the nation's first phreaks, which may or may not be true. He gives out his telephone numbers freely, will do anything to communicate with somebody (like place conference calls from his own private PBX system, provided you give him YOUR phone number), and generally will use anything you say to him against you in the future. Our advise is simple: stay the hell away from this person. Even if you haven't done anything wrong yourself, your life can still be made miserable by him if you're even suspected of having contact with wrongdoers.

This latest turn of events has saddened us — we thought Cable Pair would be a promising contributor to this publication and instead we learned a valuable lesson: don't trust anybody. Have fun, Cable Pair. Enjoy yourself. Just don't expect to see any of us over at the Chestnut Tree Cafe with you. You're on your own now.

THE TRUTH BEHIND THOSE 9999 NUMBERS

by Mark Bluebox

Once upon a time, I was talking to one of my favorite friends, one of the nation's oldest and most experienced telephone enthusiasts—some might refer to him as a phone phreak. In this particular conversation, he mentioned to me that I might want to experiment with a series of 800 numbers: exchanges starting with 9, followed by the suffix 9999 (800-9xx-9999). And so I did, and a whole new world began to open up in front of me.

They were mostly weather and time numbers in various locations throughout the country. And, since these were 800 numbers, there was NO CHARGE! One number in particular was of a great deal of interest to me and to many others. This was 800-957-9999, which hooked up to WWV, the radio station operated by the National Bureau of Standards that does nothing but tell the time and give shortwave reports. This is the most accurate clock in the entire world! You either have to tune WWV in on a shortwave receiver or dial 303-499-7111 in Fort Collins, Colorado. Yet, here I was with an 800 access! Being a bit of a shortwave enthusiast, I don't have to tell you how convenient this was for me. Unfortunately, it got too convenient for too many people.

I guess I made the mistake of giving it to a former president of a large amateur radio club in the Dallas area. He, in turn, printed it in the Amateur Radio Newsbulletin where thousands of people probably saw it. Another statewide newsbulletin picked it up and printed it. Through an amateur radio news network which this bulletin was a part of, the news got as far as California.

One day, I called up the West Link Amateur Radio News Service at 213-768-7333. (This is a service located in West Link, California that broadcasts news over amateur radio, VHF, UHF, etc.) Their latest report had this little item: "Speaking of interesting things, the National Bureau of Standards has got a very convenient time number for those of you that are not constantly at a shortwave receiver. You can dial 1-800-957-9999 for WWV. It's just another good toll-free service for us to use." The avalanche had really begun now.

The West Link report was heard on bulletin stations all around the world and, apparently, one station in Nashville, Tennessee broadcast it. From there it fell into the hands of one of the writers for the DX program on Radio South Africa! I happened to be listening to a program where they were talking about pulling in distant time stations, weather stations, etc. He then mentioned, "For those of you that live in the United States, a convenient toll-free 800 number has been provided by the National Bureau of Standards for WWV and that number is 1-800-957-9999." Imagine my surprise! Once again, the number had been broadcast all around the world. People in many, many nations now had that number. Of course, the number only worked inside the United States, but the word was being spread by shortwave listeners and QSL people everywhere.

The number was getting swamped. Needless to say, it was busy much of the time. A government official, who *also* had this number, thinking that it was legitimate, called up WWV and complained. He told them that they needed to add some more lines to their new 800 number. The general manager of the station said, "I don't know *what* you're talking about. I don't know of any 800 number that gets you WWV."

The government official told him what the telephone number was. The general manager called it and heard his own station. Astounded, he contacted the Mountain Bell Telephone Company in Denver, Colorado. They said, "You're not paying for any 800 in-WATS number. We show 303-499-7111 for WWV, but we don't have any 800-957-9999."

Mountain Bell checked it out and sure enough, the number existed but not on *their* records. No one was getting charged for this! Now, of course, you know a monopoly as well as I do—they're *sure* not going to let anyone have a free ride. So they told the WATS coordinator to find out what happened. He finally made the discovery that some technicians had hooked that number up for transmission testing. [These switching technicians are toll technicians, AT&T Long Lines switching technicians, and carrier systems technicians. In other words, they're the group of people who link switching centers together, from New York to Los Angeles, for example. In this case, the whole escapade was a kind of group effort. The switchmen and the carrier people got together and set up this number for testing, finding noisy carriers, carriers with cross-talk on them, etc.]

The WATS coordinator told them they'd better get this number off—too many people knew about it. He told them to erase *every* 800 test line number that was on the system. Not surprisingly, someone also got chewed out very severely.

So, consequently, 800-957-9999 is no longer in existence. But since then, less than two weeks later, several of the 800 test numbers have begun to defiantly reappear. Check around, you'll probably find a few interesting ones. But I doubt if WWV's brief stint as a toll-free service will ever be repeated.

Ahoy, folks! If any of you have ever used an extender that goes by the name of 8006213129, you'd better give it a call now! The people running it have a message for you.

DISREGARD THIS: 36TK109S7752A145300942211 69BR:

HACKING ON TELENET
It's as easy as 123456!

Telenet. Or, to be more specific, GTE Telenet. A massive network formed by the people and technology that were used to develop packet switching for the Department of Defense. Telenet was purchased by GTE in 1979 and has been growing in size and revenue ever since.

There are quite a few data networks in existence today. Datapac, Autonet, Tymnet, Arpanet, to name some of the better known. A data network is basically a collection of mainframes, specialized minis, and high-speed lines. Through Telenet, you can connect to literally thousands of computers, all over the country, even the world if you know the proper procedures. All this is possible by making a local phone call, in most parts of the country. [Telenet access numbers are made readily available to the public by Telenet and systems on the network, such as the Source, Compuserve, etc.]

Once your modem is connected to Telenet, you have to hit two carriage returns. You'll see:

TELENET
XXX XXX

where the first 3 X's are the area code you're connected to and the rest comprise the Telenet node identifier. You'll then be asked for your terminal identifier. Usually "D1" works for most terminals, but a simple carriage return is also accepted.

At this point you first receive the @ prompt. It is from here that you get places. And that's what's so unique about Telenet—the *way* in which you get places. You simply type a "C", a space, and the Telenet address. Then you enter the *area code* of the computer you want to connect to, followed by a two or three digit code. That's all there is to it. Telenet tells you whether or not you've found a working computer. If you want to exit from one computer and connect to another, just type an "@". You'll then get the Telenet @ prompt. Before you type the next address, type "D" to disconnect from the computer you're still connected to.

Hackers across the country have for years programmed their computers to scan the system for interesting things. All that has to be done is this: Pick the city you want to scan—let's say Boston. The area code is 617. Have your computer start its search at address 617001. If you get connected to a computer, Telenet will skip a line and print 617 001 CONNECTED. If you don't get connected, there are a variety of messages you could get. 617 001 REJECTING, 617 001 NOT RESPONDING, 617 001 NOT REACHABLE, 617 001 REFUSED COLLECT CONNECTION are a few of them. They all mean basically the same thing—there is no way to hook up to this address.

At this point, several things can be done. Naturally, you'll want to increment the address by one and search for a computer at address 617002. But how do you have your computer recognize when a connection has been made? This is necessary because you can't just keep entering C XXXXXX over and over—once you get connected, you have to enter the "@" to get back to the Telenet prompt, followed by a "D". Of course, you could type C XXXXXX, followed by "@", followed by "D" for *every* attempt, but that can get rather time consuming. It's better simply to be able to save to disk or output to a printer the addresses of connections. And, fortunately for hackers, Telenet makes that very easy.

You can either search for a string that has the word "CONNECT" in it somewhere—the only time you'd find one would be when you got the CONNECTED message. But, as we mentioned earlier, an extra line is skipped right before the CONNECTED message, for some reason. Why not simply look for that extra line? If you get it, record the address, send the "@" and "D" and increment by 1. If you don't get the extra line, simply increment by 1.

Naturally, you will be collecting Telenet addresses for informational purposes only, to find out which computers are located where, in case you ever have to get onto one in an emergency of some sort. Keep in mind that you are not *entering* any of these computers; you're merely connecting for a brief second or two. And there is no login procedure or identity check for Telenet, so you're not fraudulently using their system either.

Also, the area code system is not the only system that works on Telenet. These are simply set up to be convenient, but an address can actually have any kind of a number in it. For example, addresses beginning with 311 or 909 (the latter being Telenet's own private "area code") also abound, and there are certain to be many more.

Without a doubt, though, it's the existence of the area code system that has helped Telenet become one of the easiest data networks to hack. And until they install some sort of a user identification program, or at least have the system disconnect after it becomes obvious that there's a strange person online, hackers will continue to be one of Telenet's biggest problems.

If you have information to share with us about this or any other data network, please send it in. Requests for anonymity will be respected.

ESS: ORWELL'S PROPHECY

There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

From *Nineteen Eighty-Four*

ESS is the big brother of the Bell family. Its very name strikes fear and apprehension into the hearts of most phreakers, and for a very good reason. ESS (Electronic Switching System) knows the full story on every telephone hooked into it. While it may be paranoid to say that *all* phreaking will come to a screeching halt under ESS, it's certainly realistic to admit that any phreak whose central office turns to ESS will have to be a lot more careful. Here's why.

With electronic switching, *every single digit* dialed is recorded. This is useful not only for nailing phreaks but for settling billing disputes. In the past, there has been no easy way for the phone company to show you what numbers you dialed locally. If you protested long enough and loud enough, they might have put a pen register on your line to record everything and prove it to you. Under ESS, the actual printout (which will be dug out of a vault somewhere if needed) shows *every last digit* dialed. Every 800 call, every call to directory assistance, repair service, the operator, every rendition of the 1812 Overture, everything! Here is an example of a typical printout, which shows time of connect, length of connect, and number called.

DATE	TIME	LENGTH	UNITS	NUMBER
0603	1518	3	1	456-7890
0603	1525	5	3	345-6789
0603	1602	1	0	0000-411
0603	1603	1	0	800-555-1212
0603	1603	10	2.35*	212-345-6789
0603	1624	1	0	0000-000 (TSPS)

A thousand calls to "800" will show up as just that—a thousand calls to "800"! *Every* touch tone or pulse is kept track of and for most phreaks, this in itself won't be very pretty.

Somewhere in the hallowed halls of 195 Broadway, a Traffic Engineer did an exhaustive study of all 800 calls over the past few years, and reached the following conclusions: (1) Legitimate calls to 800 numbers last an average of 3 minutes or less. Of the illegal (i.e. phreakers) calls made via 800 lines, more than 80 percent lasted 5 minutes or longer; (2) The average residential telephone subscriber makes five such calls to an 800 number per month. Whenever phreakers were being watched, that number was significantly higher. As a result of this study, one feature of ESS is a daily log called the "800 Exceptional Calling Report."

Under ESS, one simply does not place a 2600 hertz tone on the line, unless of course, they want a telco security representative *and* a policeman at their door within an hour! The new generics of ESS (the #5) now in production, with an operating prototype in Geneva, Illinois, allow the system to silently detect all "foreign" tones not available on the customer's phone. You have exactly twelve buttons on your touch-tone® phone. ESS knows what they are, and you had best not sound any other tones on the line, since the new #5 is programmed to silently notify a human being in the central office, while continuing with your call as though nothing were wrong! Someone will just punch a few keys on their terminal, and the whole sordid story will be right in front of them, and printed out for action by the security representatives as needed.

Tracing of calls for whatever reason (abusive calls, fraud calls, etc.) is done by merely asking the computer right from a terminal in the security department. With ESS, everything is right up front, nothing hidden or concealed in electromechanical frames, etc. It's merely a software program! And a program designed for ease in operation by the phone company. Call tracing has become very sophisticated and *immediate*. There's no more running in the frames and looking for long periods of time. ROM chips in computers work fast, and that is what ESS is all about.

Phone phreaks are not the only reason for ESS, but it was one very important one. The first and foremost reason for ESS is to provide the phone company with better control on billing and equipment records, faster handling of calls (i.e. less equipment tied up in the office at any one time), and to help agencies such as the FBI keep better account of who was calling who from where, etc. When the FBI finds out that someone whose calls they want to trace is on an ESS exchange, they are thrilled because it's so much easier for them then.

The United States won't be 100 percent ESS until sometime in the mid 1990's. But in real practice, all phone offices in almost every city are getting some of the most basic modifications brought about by ESS. "911" service is an ESS function. So is ANI (Automatic Number Identification) on long distance calls. "Dial tone first" pay phones are also an ESS function. None of these things were available prior to ESS. The amount of pure fraud calling via bogus credit card, third number billing, etc. on Bell's lines led to the decision to rapidly install the ANI, for example, even if the rest of the ESS was several years away in some cases.

Depending on how you choose to look at the whole concept of ESS, it can be either one of the most advantageous innovations of all time or one of the scariest. The system is good for consumers in that it can take a lot of activity and do lots of things that older systems could never do. Features such as direct dialing overseas, call forwarding (both of which open up new worlds of phreaking which we'll explore in later issues), and call holding are steps forward, without question. But at the same time, what do all of the nasty implications mentioned further back mean to the average person on the sidewalk? The system is perfectly capable of monitoring *anyone*, not just phone phreaks! What would happen if the nice friendly government we have now somehow got overthrown and a mean nasty one took its place? With ESS, they wouldn't have to do too much work, just come up with some new software. Imagine a phone system that could tell the authorities how many calls you placed to certain *types* of people, i.e. blacks, communists, laundromat service employees... ESS could do it, if so programmed.

This was the first in an occasional series on the fun and dangers of ESS.

SOME THOUGHTS ON "GARBAGE PICKING"

Garbage picking is the art of finding things that someone else has thrown away. Hackers on time-sharing systems are long familiar with the technique of asking the operating system for some memory or mass storage space that has not yet been zeroed out, and then dumping out whatever was in there to the screen or printer. Things like password files and system programs are always updated or backed up from time to time, and that's when a "garbage copy" will be created. The alert hacker will find this if he or she looks hard enough.

You can even do some garbage picking with your own microcomputer! Occasionally, when a software house creates a disk, it copies over an entire disk, not just the programs that they happen to be selling on that disk. You might find old copies of the vendor's programs sitting in there, or all kinds of other stuff.

For those of you without computers, there are other ways you can join in on the fun. Many a tale has been told on the local bulletin boards about the enterprising phone phreaks who snuck around to their local phone company's central office early one morning and snooped through the dumpsters. In the old mechanical switching areas, you might find wires, relays, and other bits and pieces that an electronics hobbyist would enjoy. In areas served by electronic switching, computer printouts are more likely, and you might even find the garbage hoppers locked to prevent pholks like you from snooping around. Remember, other people's garbage is sometimes considered their private property. **Be sure to check with your local authorities on the legalities of digging into large corporations' back yards before you find out what the rules are the hard way.** One person who almost got into trouble over this was a New York City sculptor who was poking through the trash cans around Richard Nixon's townhouse and got picked up by the SS (Secret Service). He told the judge that he was planning to make a sculpture of the former president out of garbage, and he wanted to use the real stuff. The judge, obviously, a man of refined artistical tastes, allowed the sculptor to poke through the garbage without molestation.

Other kinds of garbage picking require some more technical knowledge and a bit of construction ability. One possibility that could keep you project builders busy is a cross-talk amplifier. For those of you who aren't familiar with the term, cross-talk (on your telephone) is when you hear another conversation (usually very faintly) underneath a phone conversation that you're having. If you build an amplifier that can filter out the background noise and amplify only the narrow bandwidth where the voice is transmitted through the phone lines, you might be able to make out what the folks are saying, for all the good it will do you. But there are other things you can hear in this electronic garbage heap. Suppose one day you hear cross-talk of a modem conversation? If you could amplify it and feed it into your computer, you would be able to monitor someone else's entire computer session. Suppose you hear someone entering in touch-tone® codes to some local call extender? All you have to do is build yourself a tone decoder (you can find schematics for these things in any Radio Shack) and figure out what the person entered. Obviously, once you are able to amplify the cross-talk to a reasonable level, your best bet is to tape-record the material so that you can experiment with the best way to feed it into the computer or tone decoder that will be further deciphering it.

There have been tales told of one enterprising phreak who built a tone decoder and then called up his favorite call extender. He then called some "dead" line (such as the silent half of a loop line somewhere; other possibilities could be a disconnected number [you hear silence after the recording finishes] or even your own phone, if you have a second line you can use) and turned on his tape recorder. It wasn't too long before he heard the cross-talk of someone else using the extender, and he picked up ten new codes inside of a week! Of course, he needed a working code to sign onto the thing in the first place, but there are some extenders where you can "hold the line open" by hitting some key every now and then. The nice thing about this kind of hacking is that you only need to make one phone call to find things out, while standard hacking requires a separate phone call for each attempt at a new code. No system in existence could detect a fellow with a tape recorder and a tone decoder listening in, although it's certainly possible that someday, someone could design their phone circuits to be 100% free of cross-talk.

That's all we have for now on the subject of garbage picking. If you come up with any more places where an inquisitive person might find some interesting information lying around, be sure to write in and let us know. Please include your method of "digging up" the garbage, and suggestions to all those other people out there who will try to duplicate your results.

THE CONSTITUTION OF A HACKER

With every generation of humans, there are certain types of individuals that emerge. There are (always have been and always will be) leaders, followers, general nuisances, etc. And then there are folks who like to play with things and figure out how they work.

Before technology came along, there really wasn't all that much for these people to play around with. And certainly there was no way for them to pool their resources except through face-to-face communications.

With telephones, of course, all aspects of human life changed. Here was a toy that *anyone* could play with and get virtually unlimited results. But of course, most people didn't (and don't) see it that way—phones are phones and nothing more. You're not supposed to have fun with them. Yet, certain adventuresome types insisted on having fun with their phones anyway. They did all kinds of things they weren't supposed to do, like figure out the way phones work and interconnect. For the first time, these technological enthusiasts posed a "threat" to technology by reaching out and touching it rather than simply using it without asking any questions.

Today there are lots of people still having fun with their phones and making all kinds of technological advancements of their own. But the real focus at the moment is on the newest "threat," people who like to experiment and have fun with computers. Not the kind of fun they're *supposed* to be having with Pacman® and Mr. Do®, but *unauthorized* fun with other people's computers.

Why do they do this? What do these people possibly have to gain by breaking into computer systems and seeing things that don't really concern them or that is of no possible use to them? In the great majority of cases, computer hackers don't gain anything material or financial from their exploration. Add to that the high risk of getting caught and it becomes very hard for the average citizen to understand what motivates these people.

Many computer hobbyists, in fact, are resentful of hackers, considering them immature and troublesome. Quite a few computer bulletin boards prohibit certain topics from being discussed, and when they do, hacking is almost always one of them. There is some justification behind this, since the image of all computer users can be adversely affected by what the hackers do.

There are also the legal people who insist on telling everyone that breaking into a computer by phone is just like physically breaking into a home or office. Fortunately, that logic seems to be shared by very few people.

In spite of all of the threats and criticism, though, the hackers are not "cleaning up their act." And public opinion, particularly among the young, seems to be in their favor, mostly as a result of media coverage.

There's even a weekly TV program about hackers called *The Whiz Kids*. Each week, this group of amazing kids has a new adventure. The scripts are a bit moronic but interesting nonetheless. In one episode, the kids (only one of which is a true hacker) find out about an evil person who happens to be stealing Social Security checks. (They discover this by casually logging into his bank account.) To teach him a lesson, they break into another computer and enter his name as being deceased. In each program, these kids break into at least one new computer. But do they ever get into trouble? Of course not. First of all, they're only children. And second, they're entering these computers for good reasons, even if they are unauthorized.

Now what kind of message is this program conveying? Apparently, it's OK to invade other people's privacy if your intentions are ultimately "good." It sounds like something Reagan would get a kick out of.

A genuine hacker breaks into computers for the challenge. He's not out to save the world, nor to destroy it. He is not out to make a profit out of what he's doing. Therefore, it's not fair to categorize him as a criminal and it's just as wrong to say he's some sort of a savior.

Technological enthusiasts operate with the same motivation that a good mountain climber has. Regardless of what may happen to him, a computer hacker will *always* be interested in playing with computers. It's in his nature. And any laws that are created to "eliminate" hacking simply won't work because of these facts. There will always be people who want to experiment with things and this urge cannot be stifled. Did hacking come to a grinding halt because of the "414" scandal? Or because of the Telemail raids? No. Judging from the proliferation of computer bulletin boards where hacking *is* discussed, it's getting bigger than ever.

The realistic way for the owners of large computer systems to look at this is to regard hackers as *necessary security checks*. That's right. Necessary because if the hackers weren't the ones to break in, who would be? Let's assume that hackers had never even tried to break into the Memorial Sloan-Kettering Cancer Center computer. Someone else would have, because the system was practically wide open. And maybe they would have had a *reason* to get into the system—to do various nasty things. But now, because of what the hackers did, the Sloan-Kettering system is more secure.

One could almost say that a person with hacking abilities has an *obligation* to try and get into as many different systems as he can. Let's get nationalistic for a moment. If you have the number for a top-secret government computer in Ft. George G. Meade, MD, odds are that the Albanians have it also. Now, would it be better for them to break into the system and find out all kinds of nice things or for you to break in and be discovered, forcing the system to become more protected? And, if you do break in, don't you deserve a note of thanks for waking them up?

Keep in mind, though, that a computer hacker is under *no* obligation to turn himself in or warn operators that their system is easily penetrable. It's the job of the sysops to notice when their computers are being tampered with and if they don't detect you, then that's a second security lapse for them.

This is a pragmatic view, however shocking it may seem. In closing, we should point out to the hackers themselves that there is no need to worry or fret if their methods or secrets are eventually discovered. This is only the beginning. Our world is turning into a technological playground.

ALTERNATE LONG DISTANCE

First of a persistent series — how the companies work and a guide to MCI

SWAGIMA. That's the word that National Public Radio uses to describe long distance services. It stands for SBS (or Skyline), Western Union (or Metrofone), Allnet (or Combined Network Services), GTE Sprint, ITT, MCI, and of course AT&T. And there are many more, each of which will eventually be covered in our pages. Right now though, we'd like to give you an idea of what these systems are and how they work.

Except for AT&T, all of the above systems work in a fairly similar manner. (This will be changing very soon and very dramatically under the terms of the Bell divestiture.) Each system has its own series of networks, i.e. land-lines, lines leased from AT&T, microwave relays, satellite links, etc. They each have local city access numbers, although some like Allnet and MCI have special ways of using a "travel" service by dialing a special number, while Sprint uses a "travelcode" to access nodes outside the subscriber's city. On others, like Metrofone, you can use the same authorization code from any of their access points.

A long distance telephone company consists of four major parts: you have your input—that is, a local access number or a toll-free "800" number to access the system. When you do this, a device called a "switch" answers, giving you the familiar "computer dial tone." When you enter your authorization code and destination number, you are routed over their network. The heart of the system is the controlling system, which includes the "switch." This is the computer that checks the authorization code, has provisions for time-of-day restrictions, travelcodes, accounting codes, and the like. They have a few provisions which the long-distance services don't appear to use, such as the infamous "speed number" recording which was a favorite of many phone phreaks (for reasons you'll soon know if you don't already). The system checks to see if the location being dialed is on the network, and acts accordingly. It makes a log of numbers called, the authorization code, and time usage which is stored on a word processing tape and then read by another system for billing. Some companies charge in one minute increments, although the system has the capability to record time usage in 6 second increments.

There are quite a few different systems in use today. A couple of the most common ones are made by Northern Telecommunications, which is based in Dallas, Texas. Another company that sells similar equipment is Rockwell Wescom. MCI allegedly is in the process of buying new switches from them, and they will be installed by Dynacomp Telecommunications, also based in Dallas.

Microwave Links

Most of the low cost services, at one point or another, use microwave antennas to transmit calls. Each microwave station is located about 30 miles from each other to make up for the curvature of the earth since microwaves travel in a straight line. Each of these stations has 4 dishes (at least). One dish is used to receive from a previous station and one is used to transmit to that station. The other two dishes do the same thing to the destination station—one receives and one transmits. So if you make a call 3000 miles away, you may wind up going through 100 different microwave stations, many of which you can see next to major highways.

This is how the alternate long distance companies manage to charge less than AT&T; they use their own systems. But this is also why, in many instances, the sound quality is poorer on the alternate services. Remember, a chain of microwave towers is only as strong as its weakest connection.

A Look at MCI

MCI (Microwave Communications Inc.) was the first new kid on the block, way back in 1967 when the idea of an alternate phone service was almost unheard of and practically illegal. MCI was first used solely by businesses who wanted to communicate between the cities of Chicago and Cleveland. That was it. And even with this amazingly limited system, MCI ran into problems with AT&T, who didn't want *anybody* trying to do what they did. Lawsuits followed, with MCI eventually getting a promise of eventual equal access to the AT&T network. In fact, MCI's legal action is considered one of the motivating factors behind the break-up of the Bell monopoly.

Now MCI is the biggest of the alternate services (they have well over a million subscribers at present, having opened their doors to residential customers a mere 5 years ago) and also one of the hardest to penetrate. The system has 5 digit codes that are entered before the 10 digit phone number, a total of 15 digits. But these codes only work from one location, making it rather unlikely to find one by guesswork. If you want to use the system from another city, you have to sign up for MCI "credit card" service which costs an additional $5 a month (on top of an initial $5 a month charge for the regular service). Here you get a list of 48 phone numbers around the country and a 7 digit code which can be used from any one of them. Most code seekers prefer scanning the "credit card" numbers since more numbers work overall. However, a strong argument can often be heard in favor of the 5 digit numbers that are located in densely populated areas like Los Angeles or New York. Naturally, the odds of finding something increase under those circumstances.

No Proven Method For Finding Codes

MCI, being the oldest of the companies, has learned quite a bit in that time. Therefore, no major bugs are still crawling around on their system. Hackers have many theories on number patterns, of course. For example, numbers like 22222 or 12345 tend *not* to work. In other words, your guess is as good as ours. As far as what they do when they know a code is being abused, MCI seems to be more interested in changing the code rather than laying a trap, as other companies have been known to do. Of course, this doesn't mean that they're incapable of doing such a thing.

MCI Features

The MCI tone sounds like all the others (a hollowish, medium-pitched, steady tone), but it has its own set of recordings, depending on what you do to it. If you enter an invalid code, you'll hear a mechanical female say: "THEE AUTHORIZATION CODE YOU HAVE DIALED IS INVALID TWO ZERO THREE" and then an ESS reorder that trips over itself (listen to it and you'll understand). If you dial someplace you're not supposed to call (for whatever reasons), you'll hear: "THEE NUMBER YOU HAVE DIALED ISNOT ON THE NETWORK TWO ZERO THREE" and the reorder. Each MCI dialup has its own 3 digit identity code and they tend to be similar the closer together they are.

Many businesses are installing MCI "dedicated lines" in their offices, which takes away the task of having to dial the MCI access number. In addition, you don't have to enter an authorization code and you don't even have to have touch-tones®. You simply pick up the phone and there's your MCI dialtone! According to MCI, you have to make at least $75 worth of out-of-state calls per month for this system to pay off. Of course, you can't access operators, directory assistance, 800 numbers, and that sort of thing because 1) MCI doesn't support any of those services and 2) they're certainly not going to let you connect to something they can't charge you for. Of course, if you know what you're doing, you can route calls in such a way that numbers that aren't supposed to go through for you will work, and God knows where it finally shows up! This doesn't involve extra codes, blasting the line with tones, or anything overly suspicious. All you need is the right combination of area codes. Now this has been proven to work with MCI dedicated lines; it's rumoured to work on dial-ups as well...

Finally, MCI is starting to offer its own phone booths at airports, which we'll report on as soon as we find one. And of course, there's MCI Mail, an electronic overnight mail service started up last fall which hackers are currently probing. When we get conclusive results on that, we'll pass them along. MCI can be reached at 8006246240.

THE FIRST ATOMIC BOMB

A TRUE TALE

This story was originally related by Laura Fermi, widow of the nuclear physicist Enrico Fermi, who, along with assorted colleagues, participated in the first test bomb in the desert outside Alamogordo, New Mexico in the early morning hours of a summer day in July, 1945.

When the date had been established for the secret test, staff members from the Manhattan Project (as the secret test was known) were invited to bring their spouses to New Mexico to watch the results of the several years of research. Each staff member had been assigned specific tasks to handle while there. Generally, they acted as observers and were stationed in a circle around the perimeter of the bomb site. Enrico and Laura were stationed in an area about twenty miles to the southwest of the bomb site.

The morning came when the bomb was scheduled to be detonated in the test. Laura told it like this...

Enrico and I woke up at 3:00 am, to go to the site. The test was scheduled for 4:30 am that day, which was July 19, 1945. We drove to our post, about twenty miles from the site. It had been arranged that the nearly one hundred of us present would be located in a circle about 100 miles in circumference surrounding the bomb site. We were all to be in communication with each other over **telephones**, all of which were connected through the exchange in Alamogordo.

We arrived at the site at 4:15 am and almost immediately it began to rain, quite a heavy, very typical torrential downpour during the summer. We waited in our car, and at 4:30 am the time came and went, but the bomb did not go off. Enrico and I assumed it might have been postponed due to the rainstorm, but decided to check with the other staff members to see for sure. For some reason, the telephone there at the site did not seem to work; the operator would not respond. *(Note: At that time, nearly all phones in the United States, and certainly in New Mexico, were manual. No dialing of any sort was possible—you had to use the operator for everything.)*

Finally Enrico decided that we would drive into town and try to contact the others and see what went wrong. So we drove back to town, and got there about 5:15 am. The only place open at that time of night was a hotel, and we stopped in there to use a pay phone. Strangely enough, the pay phone was not working either, or at least the operator never came on the line to ask what we wanted. Enrico was quite curious about all this and decided to investigate. We went outside the hotel, and Enrico found where the telephone wires came off the pole and down into the building. He decided that we would follow the wires, so we walked down the street looking overhead at the wires on the pole as we went along. Finally, we turned down one street and saw a house. The telephone poles and wires from all directions seemed to come down to this house. There must have been hundreds of wires from telephone poles all coming down onto the side of this house and going in through an opening.

We noticed that there was a front porch light which was on. The front door was open, but there was a screen door which was closed. We went up on the front porch and looked into the house. A switchboard was there, and there were a dozen or more lights on the switchboard lit, blinking off and on as people were flashing the switch hooks on their phones trying to raise the operator. The room was just dimly lit, and near the switchboard was a sofa, and a woman was laying on the sofa sound asleep! Enrico pounded very loudly on the screen door, and shouted at the woman. Suddenly she opened her eyes and looked at him, very startled. Then she looked at the switchboard. Immediately she sprang up, dashed over to the board, sat down and began frantically answering the calls...

Without saying any more, Enrico and I left, went back to the hotel where our car was parked, and drove back to our monitoring post twenty miles out into the desert. We had been at our post only about five minutes when the explosion went off, at about 6:30 am, which was two hours behind schedule. Later, we talked to the other staff members and found that there had been some confusion because of the rain. None of them had been able to reach the others because the telephone operator had fallen asleep, and the phones were not getting answered/connected...

We on the staff all had a big laugh out of it, but nothing more was ever said or done, and I doubt to this day that that woman is even aware that the first atomic explosion in the world was delayed two hours because of her.

Amazing, but true. Alamogordo was a tiny town back in the 40's, and it's very doubtful that the night operator had ever seen so much traffic in her life as the hundred or so people all on the line at once that early morning. More than likely, the poor dear had had a very rough day the day before, in the miserable summer heat, had been unable to sleep during the day, and had come to work that night thoroughly exhausted. She probably decided that "it won't hurt just to close my eyes for a minute..." and the rest of the story is already told. After all, experience had taught her that in fact she would not usually get a dozen calls all night on her shift, and she felt relatively safe in stretching out "just for a minute".

Do you have a story about computers or phones? Send it to us! If we print it, you'll get a year's subscription to 2600! The address: 2600, Box 752, Middle Island, NY 11953.

WHOSE STRIKE WAS THAT ANYWAY?

Contract talks were breaking down between American Telephone and Telegraph and the three major unions of their employees. As a result, workers walked off their jobs at midnight on August 7th. The AT&T strike was on!

We all remember the phone strike of '83. It caused us to hold on directory assistance for several minutes. It gave us many unique error messages. It made it virtually impossible to make any operator-assisted calls from all around the country. For the first time in a long while, the voices at AT&T were not answering the phone.

As we all know, a strike is an organized work stoppage by the employees in order to compel the employer to meet some demand. If the workers go on strike, it stands to reason that the company should suffer. If, for example, the union of Cabbage-Patch® producers was to strike, then none would be made, the factories would quickly be emptied, and consumers would rant and rave. If the local Cabbage-Patch® conglomerate had anticipated a strike, they could step up production, fill several hundred warehouses with millions of the surrogate orphans and, when the strike occurred, they could sell the surplus. The workers would lose their bargaining power in this case, unless the Cabbage-Patch® truckers' union also struck, or perhaps people stopped adopting the cretins, however unlikely that might seem.

This analogy leads us back to last summer when 675,000 telephone employees went on strike. A walk-out of this magnitude should have devastated any company. AT&T, though, is the exception to the rule. What AT&T really depends on are phones, wires, switching systems, computers, electricity, some optical fibers, satellites, microwave towers, and other nifty 21st century things that are all designed to run without the interference of human decision. The people are really just there to remove illegal third party phone calls from your bill, to make sure that your handwritten check matches the computer-read phone bill, or to tell you that the machine you are at cannot return your dime and that you will get a check for 10¢ in the mail. 97% of all calls made today don't use any operator assistance at all. And most of the other 3% could have been dialed without the assistance of a human. More and more "services" of your phone company are becoming *completely* automated. With ESS, customers can dial overseas direct. Android information is popping up left and right. AT&T, a leader in technology, doesn't need their workers all that much.

Glen E. Watts, president of the Communications Workers of America, said, "In 1950, for example, total labor costs amounted to about 45% of the telephone dollar while in 1980 they amounted only to 29%." John Patrick Phillips (author of *Ma Bell's Millions*) says that the company encourages or even "maneuvers" a strike. According to him, Ma Bell reaps huge rewards from a strike. Phillips, a disgruntled ex-employee, who at times compares the phone company to fascism, would have presented AT&T's organized scheme last August like this:

675,000 workers strike for about 3 weeks. 3 weeks out of a year amounts to 5.8% of a worker's salary. Let's say a phone worker made at the time of the strike a modest $250 per week (operators made $373, while systems technicians, the best paid workers, made $535).

At this time AT&T provided substandard service to the people for the same prices. The 3% loss in phone usage due to lack of operators was probably easily made up by people making an extra effort to dial direct and by the fact that some of the calls were being handled by scabbing supervisory level employees. And so, the company nets pure profit: 3 week strike x $250/week x 675,000 workers = $506,250,000!

Phillips also notes that because managers and supervisors were doing the dirty work of the phone company, these people could not work on new projects. This means that several hundred million dollars would not be invested in expenditures on new projects because there is no one to do the work. So AT&T would get interest on this money during the strike and even for some time after it was settled until work had resumed. This yields several million more dollars in profit for AT&T.

AT&T probably made out directly with over half a billion dollars from the strike. At the same time companies like New York Telephone sought to delay a $160 million rate increase so it could ask for another increase to reflect new contracts.

As part of the settlement 21 days later, top craft workers got a 5.5% increase for the first year of their 3 year contract and 1.5% for each of the next two years. They also got a $31 million training fund ($46 per employee) to help them deal with new technology and remain employable humans. All of these "gains" are subsidized by the half a billion dollars gaining lots of interest which AT&T did not have to pay to their employees. AT&T at first offered a ridiculous 3.5% increase for the first year and no increase for the next two, but after losing 5.8% of their salary by striking, workers got a 5.5% increase above the cost of living which is probably entirely subsidized by the strike itself and by rate increases.

It's certainly a nifty deal for Ma Bell. Their workers blow off steam and pay for their own raises, and stockholders don't have to worry one bit.

The strike had its effect on the consumer. As we all know, many were dialing, touchtoning®, or redialing their calls almost like usual and others were severely inconvenienced by a few managers and supervisors working as long distance or directory assistance operators often for many hours of overtime. New installations came to a standstill and many were backlogged for several months. Any emergency repairs had to be handled by supervisory personnel. But after all this, the same fat phone bill came to people's homes the next month, without any delay.

In actuality, users cannot complain to or boycott the phone company as they could the Cabbage-Patch® manufacturers, in our earlier scenario. They cannot make AT&T or their local company do anything because each customer is as unimportant as each employee. We, as customers, are all dependent on the phone. We have at least one in each home. We are billed if we use it or not, and are billed more to have it shut off for a month or two. We are all so dependent on the lines that run into our homes and on the one and a half million payphones that absorb our money that the complaints of any one or even thousands of us are quite useless. All of this utility (note the meaning of this word) was until recently controlled almost exclusively by *one* company, so in the name of human spirit, roll on with the divestiture.

THE TROUBLE WITH TELEMAIL

GTE is practically inviting intrusions, and odds are they'll get plenty

Last month, two of our reporters took a trip to National Public Radio studios in New York to reveal a very interesting development. It seems that Telemail, the electronic mail service of GTE Telenet was *still* just as easy to access as it was last year, prior to the October raids on computer owners who had allegedly broken into the system.

What had happened was this: a directory containing names of users on the Telemail system was obtained by our reporters—this list can be obtained from virtually any account on the system and, when printed out, is a couple of inches thick. They decided to go through this list and see if there were any accounts that still had the imaginative default password of "A" assigned to them. It had generally been thought, by both the public and press, that this incredibly foolish blunder had been corrected after the raids—in fact, new software *was* installed which forced a user to change their password from the default when they logged on. All new passwords had to be between 6 and 8 characters in length. But, in a system with many thousands of customers, the reporters reasoned that surely there must be a few who hadn't yet logged on since the policy was implemented.

They decided to start their search with user names that began with "B". They'd enter Telenet through an 800 number, type MAIL, and enter usernames beginning with B that were listed in their directory. For each username, they'd enter "A" as the password, and if it didn't work, they'd go on to the next one.

The first account they tried was named B.ALEXANDER. They entered "A" as the password, and lo and behold, they were in! On the very first attempt! Robert Alexander of BUREC hadn't logged in since last summer. The "invaders" were told by the system to change the password and they complied. Then they decided to have a look around.

While there was no mail to speak of in Mr. Alexander's box, they were able to access bulletin boards that this account was allowed to look at. (Bulletin boards on Telemail are simply long-term storage message bases where messages of general interest to a particular group of people are posted.) All kinds of internal memoes from the Department of the Interior were displayed.

In other words, the same old story. Nothing had really changed. Nearly half a year after seizing computers from coast to coast, the Telemail system was just as vulnerable to outsiders as it was before. Were the folks at GTE really interested in securing their system in the first place? Or did they just want to put the fear of the lord into hackers?

At first, when this story was breaking, GTE tried to deny that such a break-in was even possible. It had to be an inside job, they claimed, because nothing is wrong with our system. Then, when it finally started to become clear that this break-in did occur and that it was because of the default passwords once again, GTE took the expected step of blaming the customers. "We're not responsible for maintaining the security of the accounts," they said. "That's up to the subscriber," in this case, the Department of the Interior.

So, our two reporters came up with a plan. What if it hadn't been an outside agency's mailbox, but one belonging to GTE themselves? Who could they blame then?

They went to the letter "D" this time and searched for accounts that were affiliated with GTE. The first one was D.CORCORAN and, once again, they got right in. And Denise Corcoran of GTE had access to literally hundreds and hundreds of bulletin boards with names like PAYROLL, GOVT.AFFAIRS, and JAPAN.

On top of all this, it took GTE nearly a week to close access to these accounts, even after they were exposed on nationwide radio.

What our reporters proved here is that Telemail is either unable or unwilling to protect its customers. Unable? That hardly seems likely. After all, most computer bulletin boards run by high school kids are able to protect their users' accounts from outsiders. Why can't one of the largest and most expensive electronic mail systems do the same? Apparently, what we have here is a company that has grown too big too soon, and is now unable to overcome the inertia that its size has created.

How to Really Have Fun

Once a hacker manages to get into a Telemail account, he's really set. By typing DIR " at command mode, he can get a listing of everyone that the account is allowed to see—their username, full name, company and division, and user number. He can see *any* user if he figures out their full username or user number. Typing DIR USERNAME or DIR USER NUMBER will give all of the above information about that person, if he exists.

From the huge list that DIR " generates (which takes a couple of hours to print at 300 baud), a hacker can scan for passwords that are defaults, first names, last names, usernames, or company names. Some GTE test accounts, for instance, used to have a password of GEENOGTE.

Telemail allows three logon attempts per access. Telenet allows four accesses per call. So each call to Telenet will yield 12 logon attempts to Telemail. Judging from the huge amount of users on the system, finding an easy password doesn't take all that long.

There are all kinds of neat features within Telemail accounts that seem to be exclusively beneficial to hackers. If the account has access to the SET command, the user can tell the system not to print a welcome banner on logon. The information that's printed on the welcome banner tells the user when his last access was. If a hacker arranges for that information not to be printed, the *real* user won't find out that his account was being used at 3 in the morning. And odds are that he won't really notice the absence of the message—if he does, he'll probably blame it on Telemail.

Then there's the UNREAD command. This actually allows a person to read through someone else's undelivered mail, and put it back when they're finished without anyone knowing that it's been read (unless a message was sent with a return receipt, which is rare). Telemail, it seems, practically bends over backwards to accomodate hackers.

What's so great about having a Telemail account? Why should a hacker spend all this time getting one? It's another means of free (or cheap) communications. All one has to do is call Telenet, enter Telemail, and read or send messages that can be *unlimited* in length. He can share one account with someone else (which is the least risky way to work things) or communicate with another usurped account that's allowed to send to and receive from his account. This is naturally a bit more risky since if one account is reclaimed, both may end up being taken down. Transmission of messages on Telemail is instant and there's never a busy signal. More importantly though, Telemail seems to be beckoning the hackers to come back home.

(Shortly after this article was dispatched, we received word that Telemail no longer uses "A" as a default. Whether this is true at all, whether they're now using a default of "B", or whether they're using defaults period, is something that hackers will no doubt find out soon. Drop us a line if you find out anything.)

A TRUE SAGA OF TELECONFERENCING

by Electric Moon

"God, I wish I had a box," David said. "I can see it now. I bump off Information in Wisconsin and get an empty WATS line to play with. I keypunch a few multifrequency operator tones, and ta da! It gives me a conference. But I can't do that anyway, since I'm on ESS."

"David," I responded, "I know this sounds stupid, but I don't understand a word of what you just said. Okay, this is what I know from the conference: with a blue box you make tones of certain pitches, so that the phone thinks you're an operator. That way you can make long distance calls for free or start a conference."

"Very good."

"But what's ESS?"

"Anyway," David said, "it's easier and safer to use an extender to call long distance than to box."

"*But what's ESS?*" I repeated.

"Okay, here we go. The famous Smith briefing for beginning phreaks. Fasten your seatbelts, ladies and gentlemen..."

"I resent being called a beginner," I said.

"In the history of our great phone system, Ma Bell has undergone many changes. In her youth, she was made up of so-called step-by-step systems. These were lovely and easy to circumvent, but noisy and slow. Also, 2600 Hertz disconnects a step system, so you can't box off of one. Most of these were switched by hand by small-town operators. Then someone came up with crossbar switching, and Ma Bell made little clicking noises all day long as she switched almost automatically.

"But, horror of horrors, Ma Bell finally got old. She grew senile and paranoid. In order not to forget things, she wrote them down. Every time a little customer called a number he shouldn't have known, she wrote up a trouble card on him and filed it neatly away. This system was noiseless and easy. Soon Ma came up with better security measures, longer customer records, and tighter filing cabinets. She buried light-fiber cables, and everyone knows you can't splice two light-fiber cables together. She changed her own phone numbers regularly, and computerized everything. Each change came about slowly, but the final product was ESS. So the main phone systems are step, crossbar, and ESS."

"Which one am I on?" I asked.

"I don't know. Some people can tell by listening to the ring or the busy signal, but I can't," he admitted. "If you can get call-waiting, you're on ESS. Call Customer Service and ask."

***

We talked on conferences almost every night for two weeks. Napoleon Bonaparte set them up, and we talked to the Hacker, Cracker, Tom Keevis, and Max Wilke.

I learned a few things from conferences, and a lot from David. He told me about the Michigan loops. Apparently, if I called a certain number, some stranger would pick up the other end and we could talk. How stupid. Then David explained that the other person was calling a phone number too, and we'd get connected somehow. A loop around here was 424-9900 and 424-9901. If I called one end and someone else called the other, we'd be connected. This was useful if we didn't want to give out our phone numbers. In Detroit, lots of people—not only phreaks—know about loops. If you call up one end of a Detroit loop, someone else is likely to call within five minutes.

"You never know who you'll get," David said. "Hacker and I call and wait, and sometimes homosexuals get on and say, 'Looking for guys?' or girls get on and say, 'Guess what color underwear I have on?' But you also get other people—car salesmen, teenagers, and college students—lots of college students."

He gave me some Michigan loop numbers and I started calling them through extenders. I talked to a lot of weird people and a lot of normal people. I also called some pay phones in Berkeley and Carnegie-Mellon, and talked to whoever answered.

The Phreak was my idol. He was the idol of most of the phreaks I knew. Lots agreed that he was the best phreak and hacker (okay, little did we know then). He was only fourteen years old, and lived in Boston.

One day I called up a Michigan loop and heard a lot of static and clicking. I also heard some people talking—mainly two boys. One of them had an unmistakable Boston accent. It was Steve the Phreak.

"Hey Phreak," I said. "This is Electric Moon!"

"Hi Electric," he said. Then he asked his friend, "Should we keep her?"

"Yeah, what the heck!" said the anonymous phreak. A beep signalled the departure of the Phreak.

"Where'd Steve go?" I asked.

"Off to look for more loops, the idiot," said the boy. "It's too loud in here already."

"What's your name?" I asked.

"I'm Ivanhoe. I'm a Steve too, but you can call me George."

"What?"

"To differentiate between me and Phreak."

"I'll just call you Ivanhoe," I said. "Where're you located?"

"I'm in California. I'm seventeen. And you?"

"I'm in Ohio. I'm sixteen. Call me Electric." I suddenly realized I was yelling above the din of the loops. The Phreak kept putting on more and more. The loops themselves made clicks and static, but the people on them made it even worse. They couldn't hear us and they couldn't hear the people on the other loops, so they loudly chatted away.

Every time Ivanhoe or I heard the Phreak beep on or off, we screamed at him to stop adding loops, but he pretended not to notice, and continued at a rate of six or so a minute.

Finally I couldn't take the noise. I yelled a loop number to Ivanhoe, and we ducked out.

"Hello?" asked a quiet, low voice.

"Hi," I panted. "Thank God we're out of that mess."

"Yeah. He'll probably have it up for a few days before they figure it out," Ivanhoe said.

"He's crazy," I said

"Yeah, but he knows a lot. He still has a long way to go, though. He has to learn to be careful."

"I know." I tried to act experienced. "Boxing a conference from his home is incredibly stupid."

"Have you heard him on Autovon, though? He's a riot, but I'd never do what he does!"

"What does he do?" I asked.

"He'll have to show you," Ivanhoe said.

Click! "Emergency break from G.I. Joe. Will you accept?" asked the operator.

"No," we said in unison. I smiled, imagining the shocked operator. She probably thought his mother was dying.

"No?" she asked uncertainly.

"NO!" we yelled, and laughed as she clicked off again.

"Well," Ivanhoe said, "that must be Phreak. He probably wants me to call him. I'll tell him to start another conference."

"Okay," I said. I hung up the phone and walked into the kitchen. I set my notebook and pencil on the kitchen desk and took a cold apple from the refrigerator. The phone rang as I crunched the first bite.

"Hello?"

"Hi. Anyone you want to add?" asked the Phreak.

"Sure. Add Trader Vic."

"Okay," he said. I heard a beep, silence, the people talking.

"Quiet down, everyone!" Ivanhoe said. "The Phreak is going to show off, but what he's going to do is pretty dangerous."

Beep-beep! Beep-beep! The Phreak had brought Trader Vic on.

"Hey dudes, what's going on?" he asked.

"Shh!" we said.

"You can't hang up on them once they're on a conference," said Ivanhoe. "If someone suspects what we're doing, we'll have to hang up the whole conference."

The Phreak beeped off. He was back in a minute, talking officiously.

"Yes, I have a Flash Override call for location four-zero-two-niner," he said calmly.

"Flash Override? Who is this, suh?" asked a deep Southern accent.

"This is General Watt." The Phreak had to make the guy believe he was a Joint Chief of Staff.

A nasal tenor came on the line, heralded by an amazing overture of clicks, beeps, and tones.

"General, for whom are you placing this call?"

"For Ronald Reagan," said the Phreak. I felt like I had been stabbed. What an idiot! But I couldn't hang up, because the operator would hear the beeps. I listened instead.

"Ronald Reagan?" asked the voice disbelievingly. "Sir, what is the code on this call?"

"I'm at the White House right now," said the Phreak cooly. I knew he was stalling for time as he flipped through stolen Autovon manuals. "Sergeant, I have the code right here. I'm at location C-one-four-six-two-D, placing a Flash Override for Timberwolf to location four-zero-two-niner. The operation code is zero-fiver-zero-niner."

"That is correct," the operator said, and I could have hugged the Phreak. "Please hold, sir, and I'll put your call through."

Beep! Beep!...ker-chunk.

"Andrews Air Force Base," said a woman. "General Hodge is out right now. Should I sound his beeper?"

Silence. What now? Two people spoke at once. Trader Vic broke through loudly.

"Yeah, like, this is a conference call, and we just, like, wanted to see how you were doing, you know?"

"Excuse me?" asked the startled woman.

"I'm sorry," I interrupted quietly. The time had come to try and salvage this thing. "I'm the White House internal operator, and we seem to have given the wrong location identifier. Thank you very much."

The General's secretary clicked off and our nasal operator clicked on. "What seems to be the problem, General?" he asked.

"I'm sorry," Ivanhoe said. "The President decided not to make the call after all. Thank you, though."

"Yes sir, thank you," the operator said, and clicked off. We held our breaths until we heard the final beep-beep.

"Vic, you idiot!" I cried.

"What?" he asked. "I thought it was pretty funny!"

"Funny, my foot," Ivanhoe said angrily. "That was a stupid thing to say. And Steve, why didn't you answer?"

"My mom called me and I had to go take out the trash," said the Phreak.

"Phreak, you're crazy," I said.

"I know," he said in his deepest Boston accent. "But you all love it."

***

A week later, the Software Pirate called me and said the Phreak had been caught. I called Ivanhoe, who told me that Steve was visited that morning by three FBI and two Bell Security agents. Ten other people were also caught. The FBI woke all the boys up at 6 AM so they wouldn't have a chance to warn friends.

As soon as school was over, the Phreak called Ivanhoe and told him all this. He waited an hour until it was 4:00 in Utah, and called the Software Pirate, who called me.

The news spread among phreaks and pirates so that anyone involved knew about it by dinnertime on the East Coast.

Late that night, the White Knight set up what we thought was the last conference. Ivanhoe, David, Demon Diode, and the Cracker all expected they would be caught.

We called the Cracker and asked him to talk.

"Why not?" he said dryly. "I'm just sitting here waiting for the FBI. I have nothing better to do."

They got him the next morning.

(The names and locations used in this story have all be changed, so

The Simple Pleasures of a Step Office

There are still more than a few step offices in the United States today. Most of them are in rural areas, but there are still a few cities (mostly in the south, southwest, and west areas of the country) that have step. These antiquated telephone systems can best be described as a bunch of relays and wires—clicking and stumbling over themselves.

It's easy to find out if you're in a step office—especially if you're using a rotary dial phone. (In many step areas, that's all you *can* have, particularly on the east coast since they don't have what's known as common control, which allows for touch tones®. Some offices have been converted, however, using some sort of tone to pulse converter—every time you hit a tone, you hear it being pulsed out.) With a rotary dial phone, you can hear the actual switching. If, say, you're dialing 675-9112—you'd dial a 6 and you'd hear what's known as the selector kick in (more on that later) with a kind of a clunk. Then you'd dial 7, and hear a second thing kick in with a mild click—that's what's known as the digit absorbing relay. Depending on the office, this relay can kick in on any or none of the numbers. What it does basically is absorb an extra digit which is only needed to make the telephone number 7 digits long. So, in this case, the second digit of the number, which is 7, is the extra digit. You would probably be able to substitute any number for the 7 and still have the call go through, since that digit is ignored. Some offices absorb two of their digits, which means that they had five digit phone numbers before uniformity struck. To continue with our demonstration, you'd next dial a 5, and hear another click at the end of your dialing sequence. After dialing 9, you'd hear click, pop, snap—several things kicking in, then the 1, clunk-clink, and then the last two digits which wouldn't produce any sounds at the end of them. Then it will go into a ring cycle, assuming that's a valid number in the office.

Step offices usually have a very mechanical sounding ring, similar to crossbar. Ring generators, though, can make step sound like ESS. Often you hear what sounds like a busy signal or static in the background as the number rings. An easy way to tell if you're dialing into a step office is to try dialing XXX-1111 and see how long it takes to get a ring or reorder or whatever. Then try calling XXX-0000. If it takes more time to get to the same point, it's a step office because step is the only system that actually pulses out the numbers all over again.

A Phreaker's Delight

It's much safer to blue box and phreak from a step office because they're very basic, crude offices with no safety features (safety for them, that is). And if you're lucky enough to live in a fairly large metropolitan area that's still on step, you might dial up a number that you know is ESS from your step area and flash the switchhook. You'll get what's known as a wink. That's the equivalent of whistling 2600 hertz for about a half second to reset the trunk. You'll hear a click-click. That's your cue to put in various multifrequency tones (KP+number+ST). 2600 hertz is not needed at all, and since that's the tone that usually sets off alarms, this is a very safe way to blue box. (Incidentally, this occurs more through a flaw with ESS and not step.)

If you *really* know what you're doing and you know a few things about step switching, you can, on a touch tone® phone, dial up a number and listen in the background for the switch level. Let's say you're dialing 941-0226. You won't hear it rotary dial *those* numbers, but you *will* hear another number or series of numbers in rotary step pulses. That's the selector we mentioned earlier. Let's say that after you dialed 941-0226, you heard a 5 being pulsed out. What does that mean? The selector is the decision-making part of the phone call. Different prefixes are stored in different levels in each central office. In this particular case, 941 happens to be stored in level 5 in whatever office you're calling from. There's no rhyme or reason to it; the selector level could be anything up to three digits in length. (If it was three digits, you'd hear each individual digit get pulsed out.) The toll center is usually level 1 and the operator is usually level 0. So what can be done with this information? If, after dialing 941-0226, you enter your *own* rotary five, you'll once again hear the click-click which is your cue for MF tones.

While step offices have no special phone phreak trapping capabilities, they are just as dangerous as any other office as far as being traced. They have what's known as trap and trace. If a certain person (or computer) is being harassed, they'll put a trap plug on that particular line. If you happen to call into that number, you won't be able to hang up until the other party does.

Some More Tricks

In some step areas, local calls are limited to certain exchanges that have the same first digit as yours. For example, the 222 exchange can dial 235 and 263 as local calls. But in order to call the 637 exchange, you must first dial a 1 which makes the call non-local. If you dial a 6, you'll get an immediate reorder. But somewhere between you and the 637 exchange, is the 231, 233, 235, and 239 exchanges. There's no 237. So you dial 2. Clunk-clunk. You dial 3. Click. And then you dial 7. Ching-clunk. It goes to the 637 exchange! Similarly, a 281 from the 287 exchange could wind up in 471. Why? Because these numbers are all coming from the same switching center. That just happens to be the way step works (and in some cases crossbar). If you could seize the 222 trunk, you'd enter KP+25500+ST to reach 222-5500. To reach 637-5500, you'd enter KP+75500+ST.

Then there's "step crashing"—if the number you're calling is 675-2888, and it's busy, you can dial 675-2887, and in between the last pulse of your rotary dial and the time it would start to ring, you can flash your switchhook extremely fast. If you time it right, you'll hear an enormous loud click on your end. Then, all of a sudden, you'll cut into your party's conversation. (This works because of step's relay system. One relay has determined that the line you dialed is open. Then, before a second relay sends along the ring pulse, you throw in a 1, which jumps the number you dialed up by one, and fools the system into connecting you to a busy number.) There is one drawback to this, though. You, the party you've crashed in on, and the party they were talking to are all stuck together until you all hang up at the same time.

If you're in a step office where 411 is used for directory assistance, chances are that there are test codes in the format of 11XX. 1191 might be ringback, etc. In such places, dialing 1141 will also get you directory assistance, but at no charge! In some of the newer step offices, 410X is the format for tests. There, you can dial 4101 for free directory assistance. Other test numbers are (usually): 4100—off-the-hook recording, 4102—test board, 4103—miscellaneous, 4104—ringback, 4105—disconnects your line for about 5 minutes, 4106—various tests, 4107—pulse test, 4108—test board, and 4109—your telephone number in touch tones®.

Different Varieties of Step

There's more than one kind of step office. We've been talking about the most common type, used by both GTE and Western Electric (Bell). It was invented by Automatic Electric early in the century. 214-381 is a typical Bell step office (note the reorder in the background of the ring) while 214-256 is a typical GTE step office (the ring sounds like it's underwater). For both of these, a suffix of 1798 will always provide a busy signal, free of charge.

There is also something known as XY step, which is strange, unusual, and for the most part put together very poorly. It looks similar to a crossbar in appearance. Instead of a round switch, it's tall and rectangular-shaped. To dial a number, it moves up and across a ladder of contacts, as if it was a piece of graph paper, hence the name XY. On these systems, the last digit in the phone number is usually up for grabs. You can accept collect calls on a number with a different last digit from yours. The calls will still reach your number, but it won't show up on your bill. Also, suffixes beginning with 9 and 2 are usually interchangeable. A typical XY step office is 518-789. A suffix of 3299 will get you a standard step test.

Great Britain uses the Stroger system and there is also the all-relay step, which is *very* rare. It was developed presumably to save switches. One such system exists in Heath Canyon, Texas with only 36 subscribers at 915-376. A neighboring town that's also all-relay can be found at 915-386.

If you'd like us to tell you something about a particular exchange anywhere, send us the info. We'll investigate and print the results.

IBM'S AUDIO DISTRIBUTION SYSTEMS SURE CAN BE FUN!

One day several years ago, a hacker was doing some routine 800 number scanning on his touch-tone® telephone. This has become a very popular pastime because it's totally free and not easily defined as illegal in itself. Usually, what somebody does is zero in on a particular 800 exchange and dial many different numbers (often in sequential order), jotting down the interesting ones. That's exactly what this person was doing when he made a most interesting discovery. After hearing literally dozens of modem tones, and "Doo-Dooo-DOOOO! The number you have reached," "Eastern Airlines, can I help you?" and "Special operator, what number did you dial?" messages, he heard a recorded female voice say, "Please keypress your last name." After a millisecond or two, he looked at the letters on his touch-tone® buttons (never get a phone without those letters), and started to spell out a name. Another recorded voice read back someone's full name and then the old voice came back and said, "Please keypress your password." He suddenly got an idea and spelled out the person's first name. It worked! He had broken in—to something.

What this person found that day (and what many others have been discovering ever since) was an IBM Audio Distribution System or ADS. Nearly every IBM regional office has at least one of them. Operating out of an IBM Series I computer interfaced with a telephone switchboard, their original purpose was to provide a fast, easy way for IBMer's to contact each other without playing "telephone tag." All a subscriber has to do is call the system, login, and leave or receive aural messages. Commands are entered using touch-tone® keys (*R—record a message, *T—transmit a message, *L—listen to a message, *C—customize certain features, *D—disconnect are the main commands. By pressing a 9 or a #, brief help messages can also be heard.). No computer terminals were needed here. Nearly *anybody* could figure out how to use the system.

Fortunately for hackers, IBM people were both careless and apathetic. Many of them had very easy passwords and others never used the system at all, even though they had been assigned accounts.

So guess what happened? Friendly tech enthusiasts found their way into these systems and grabbed accounts left and right. Many of them set up impromptu networks where they would exchange technical information, phreaking news, stories, anything! (Sort of like a computer bulletin board, except that your voice is your keyboard. This proved very beneficial to those phone phreaks that hadn't integrated themselves into the world of computers—here was a computer that could be played with without the requirement of a terminal and modem, as well as the means to communicate with computer hackers for the first time.) Messages could be as long as eight minutes or as short as three seconds. Users could, by entering commands, adjust volume and speed, classify their messages (personal, confidential, personal *and* confidential, or internal use only), create distribution lists, change their status, etc. In short, the ADS has become a favorite toy of phreaker and hacker alike.

There are hundreds of ADS's all around the world, with more being plugged in every day. IBM is selling the systems to other companies, who then use them for their own employees, or lease accounts out to other people. IBM tells us that the price for a system with a 1000 user capacity is about $110,000. Financing terms are available, they say.

It is quite reasonable to assume that every ADS that is presently operational has at least a few usurped accounts on it. Even systems in Italy and England are being mercilessly invaded by American crackers. What's particularly funny about all this is that IBM has no way of knowing whether the users of the system are legitimate or not, since the software is written to prevent eavesdropping, even from the system operator's account. It is also impossible to find out what somebody's password is, without being in that person's account. As one IBM executive told us, "As long as they don't do anything outrageous [like send abusive messages to other users] and the legitimate user doesn't tell us that his/her account is being used by someone else, we'll *never* know they're in there."

Needless to say, some high-level administrative meetings dealt with this problem. For IBM, things were starting to get out of control. One group of phreakers had so many different systems under control that they started to color code them. Rumour has it that they ran out of colors and were forced to buy a jumbo box of Crayola Crayons® to find out the names of more. On the East Coast, a system was so heavily inundated with unauthorized users that it was commonly believed that there were more of them than legitimate users. And, somewhere in Italy, Midwest accents slowly started to abound on that country's sole system.

IBM began to make some drastic changes. To prevent intrusions from occurring in the first place, many of the systems were programmed to delete an account if it wasn't used within a certain period of time or if the password had not been changed from the system default (the first letter of the last name repeated three times). In an attempt to get rid of those that had already broken in, they started to look at their 800 number userlogs, to see which accounts were constantly being logged into on the toll-free line instead of the local number or the IBM internal tie-line number. A company employee wouldn't have to use the 800 number unless he was on the road. But, they reasoned, a phone phreak would.

On this, of course, they were completely wrong. A phone phreak can make a call to anywhere he damn well pleases without spending a cent. A few even managed to access the IBM tie-line! Good phreaks, to avoid suspicion stopped using the toll-free numbers.

IBM reset passwords on suspect accounts and then went in to see what other names were linked by "reading" distribution lists and seeing what other names were being communicated with. The intruders answered this by deleting their distribution lists and erasing all old messages.

This battle of wills is continuous. One system operator in Los Angeles attached a recording that told anyone who failed to login after three tries that their call had been traced. She later admitted to *2600* that this was simply a scare tactic used out of desperation.

Ironically enough, some of the worst offenders—as far as leaving doors wide open—are the system operators themselves. A few operators have left their privileged accounts' passwords set to the default (three zeroes). This allowed an intruder to come in and use the special "star-zero" command, which allows *system* messages to be changed. (These are the messages that tell the subscriber what to do next, etc.) "Please keypress your last name," could easily become "What the hell do you want?" There are hundreds of messages and oftentimes pranksters would change only the most rarely heard ones, to add to the surprise of the user who wound up hearing it; "Your message has reached the maximum length" was reportedly replaced by "You have spoken for too long and you may not speak again." Any user's password can be reset to the default from the operator account, so entry to all accounts is indirectly possible after cracking the operator account. Brand new accounts, though, are created offline.

If you like keeping in touch, an ADS may be just what you're looking for. With this system, your phriends are always reachable, no matter where they are.

Unless they've left the magical land of touch-tones®.

THE WOES OF HAVING A SMALL-TIME RURAL PHONE COMPANY

This story is for those of you who hate Ma Bell with a passion. In many parts of the country, Bell is not the company that provides you with telephone service. There are lots of tiny telephone companies out there and some of them make Bell (and her children) look pretty terrific. The following is from one of our readers who has to put up with a rural telephone company.

I had a problem with my telephone company. I picked up my line, and there was a dial tone there. I began to make a long distance call. After the tenth digit went through, I heard: "do weee doo... We're sorry, your call cannot be completed as dialed. Please check the number before dialing again or call your business office for assistance."

So I switched to my good phone which makes clean crisp tones and dialed the same number again. I got the same message again! I said, "What the hell?!" (It was an 800 number, of course.) So I switched over and dialed a regular "1 plus" number—I started dialing the number direct: the same recording came on!

So I dialed my local business office which is the repair service. It was a local seven digit number. Again, all I got was: "do weee doo..." Then I dialed up the operator and waited a second or two and the recording came back on.

I had an idea. "I know what they've done; they've made a mistake in the central office and changed my touch tone rating to rotary!" Doing that would certainly produce the effect I was getting. If you tried to break the dialtone, you couldn't call anything because it's not programmed in. They must have made an error somewhere. I picked up my rotary dial phone and I dialed the local repair service again. But it did the exact same thing on the rotary phone!

So I tried calling a local number (local to my exchange) and got the recording. *I dialed my own number!* "Your call cannot be completed as dialed." I tried 411—same thing. I dialed 611, the old centralized repair service that had been phased out in my area but which rings in a distant city served by the same telephone company. An operator said, "Can I have the number you're speaking from?" and I told her; "Thank you," ring, ring, ring, click, "This is telephone repair service. Can I have the number you're reporting, please?" I gave her the number. "Oh sir, I'm sorry, that number is no longer served by our repair service. You'll have to call your local repair service number," which was the one I couldn't get through to. I said, "Operator, I tried calling that and I got a recording saying the number I called cannot be completed as dialed." And she said, "Well, I'm sorry, you'll just have to call and report it to your office." I said, "I cannot! Can you pass this information along to *my* repair service? There's something wrong with the phone line—it only dials you." "I'm sorry, I'm not allowed to do that. I *can't* do that."

So I hung up and called 611 again and the first operator popped on the line again, and I said, "Operator, I'm not going to give you the number I'm calling from—I'm having a very difficult time. I called repair service, they were nasty and hateful and wouldn't respond to getting my phone fixed." I told her I had to call my local repair service, but was physically unable to. I asked if she could call it for me. "Certainly, I'll be glad to. What's your phone number and I'll call you back." I gave her the phone number, waited about 40 seconds and called her back. I asked, "What happened?" She said, "I got a recording when calling your number saying that my call couldn't be completed as dialed." "OK, that's the problem, anybody trying to call my number gets that recording—anything I try to call *gives* me that recording." "Well, let me try to ring repair again."

We ring repair service and get the *same lady* again. "Sir, I *told* you you're going to have to call your own repair service. Don't bother me with this anymore! I've told you we cannot help you here." I said, "Don't you have a phone there?" "Yeah." "Can't you pick it up and call my local repair service number? It's a seven digit listed number, can you not call it?" "*No*, I cannot! It's not my duty; it's not my job. You should be able to do this yourself. You're going to have to go down to the repair service or use a [semi-]convenient pay phone," which is 10 miles away. Hell, the repair center is closer!

I got in the car, red-faced with hysteria, and I drove in and called repair service from inside the telephone building. I went into a door marked "Employees only!" I just picked up the phone; no one was there. A person picked up and said, "Can I have the number you are reporting, please?" I yelled, "NO!" "What are you calling me for?" "I want to talk to somebody in person about my problem. I've got a terrible problem and it cannot be handled over the phone. Please come down the hallway—I'm somewhere in your building."

She came in and I explained to her the rude treatment I got from centralized repair service. "I'm terribly sorry that happened... OK, you're going to have to come into the business office. Just go down the hall. Talk to one of our well trained service representatives, and they will help you." "Why can't *you* help me—you're the repair service!" "Just take this form and hand it to the lady at the desk."

I went to one of the service reps and went over the whole story again. While I was telling her this, I noticed a 75-year-old senior citizen right next to me talking to *his* rep. He had a very similar problem. He was getting nowhere. And I said to him, "You might as well take your telephone and throw it in the river, because you're not gonna get any service out of these people! They are the sorriest human beings that ever drew a breath. They don't give a damn about you. They certainly don't give a damn about me!" (I'm now yelling at the top of my lungs, by the way.) I said, "These people don't give a shit about anything except collecting their paychecks. You might as well just leave!"

All of the people in the telephone company were looking at me: all the customers, all the business reps. And I told them, any time I report anything there, I get treated like some sort of an asshole. For instance, two weeks earlier I had reported that pay phones in this particular prefix wouldn't dial 800 numbers. If you dialed an 800 number, you got a request to put in a 25¢ deposit. When I reported *that*, they said, "Yes, you must pay for your 800 number, like it was a local call." (You won't get your money back from the phone—they are Northern Telecom phones that don't have a return coin slot, so it can't give you your coin back.) I had told them, "It is a *toll-free* 800 number, hence the word 'toll-free'. You do not have to put in a quarter." All of the representatives said, "No, you've got to put in a quarter. You must pay for a toll-free 800 number."

Well, to make a long story short, the young lady was so upset that I was yelling and screaming at everyone in there, that she took my record, dashed out of the room, came back and said, "I'm terribly sorry to have inconvenienced you. I'm sorry that you're upset—I notice you're red in the face. Your phone will be turned back on before you get home. It was just an error. Someone didn't pay their bill and it was one digit away from your number and it was all a mistake."

The next day, I spoke to the vice president of the phone company and told him about my problem and the 800 incident, as well as a whole collection of other things that shocked and upset him. He said he was very grateful to me, and would consider hiring me as a consultant.

Since that episode, things have gotten better. 800 numbers are now toll-free from payphones and the repair service is a little bit better. But there are still plenty of problems almost every time you dial.

You might say that it takes a phone phreak to straighten out a phone company. You might also say that Bell never looked so good.

ARPANET HOPPING: AMERICA'S NEWEST PASTIME

What is ARPANet?

ARPANet (Advanced Research Projects Agency Network) has been around since the 1960s. Its intentions were to link many computers together in order to share resources. The various research projects on ARPANet involve both major universities and the United States military (the two are closer than either would care to admit).

Up until last year, ARPANet was one big happy family of military and university computers. Then, in view of *War Games*, etc., it was decided that perhaps the military would be better off on their own separate network. And so, MILNET was established.

This proved to be very convenient for hackers, since they now *knew* where all of the military computers were—all it took was access to MILNET in order to play with them.

Since ARPANet can communicate with MILNET and vice versa, all kinds of interesting possibilities exist. Elaborate routing makes it easy for a hacker to cover his trail, in much the same way that a phreak routes calls through three different long distance companies to protect his/her identity.

Where can dialups to ARPANet be found? All over the place. For one thing, many numbers are in circulation among hackers. For another, they're not considered all that much of a secret, since the numbers by themselves don't allow you to logon.

If you know of a major university computer, there's a chance that it's already hooked into the ARPANet. If this is the case, HELP files will be readily available on that system to explain how to access the network.

The network itself is an entire world waiting to be explored. Ironically, many sensitive computers that are "not accessible by phone lines" *are* accessible by ARPANet! There are a lot of lessons that still must be learned, it seems.

So Simple A Child Could Do It

Moving around ARPANet is very easy as almost any hacker that has used it will attest to. It was designed upon the principle that people on one system should have easy access to other systems. "Easy" is the key word here. If a direct ARPANet dialup is being used, there shouldn't be any problem. If a MILNET dialup is being used, you will need a TACID, which is a private authorization code.

The word ARPANet is used to denote all networks. There are many networks (see *2600*, May 1984), but all can be accessed as one through "gateways", which are basically windows into other networks.

How It Works

There are two basic commands that can be used on the ARPANet: "@o" and "@c". "@o" *opens* a connection with a host. (For example, @o 26.0.0.1 will connect you with a host hooked to ARPANet—indicated by the 26.) Finding addresses is really the only hard part. At one time, a few systems had a HOST command that would give you a complete listing of hosts, and their addresses. In fact, this command is still on many systems but what was unique here was the fact that you could run the program *without logging in!!* Apparently, they got wise to hackers, and fixed HOST so that it only works from logged in accounts.

After typing "@o", the network will respond with "Open" or, if the attempt was less than successful, a self-explanatory error message such as "Bad" or "Destination host dead". When you get the "Open" message, that means you are now connected to the host computer and you can do whatever you want, like login, read help files, etc. Communication with the network is not cut off, however. The network is always there, waiting to be spoken to. Commands to the network must begin with "@". For example, type "@c" when you want to close the connection with whatever computer you hooked into. This will probably take a moment or two, since the network has to close up a few things before it can transfer control back to you. (Incidentally, if you need to send a command to the remote host that contains "@" in it, simply type an extra "@" next to the first one and ARPANet will ignore it.)

Some Safety Tips and Interesting Programs

If you can dialup to a host that is connected to ARPANet, and you have an account on it, this is ideal. There is a good chance that the host will support a terminal simulation program, that when supplied the host name that you wish to communicate with, will connect you to it through ARPANet. It will then seem as if you're on a terminal connected to that remote host. To close the connection, you will have to read the documentation on the host that you dialed up to, since it changes from system to system. Naturally, using a local dialup to access a host instead of going through a MILNET or ARPANet dialup is much "safer", since you are not accessing ARPANet directly.

Another feature of ARPANet is the FINGER command available on most TOPS-20 systems, and many other types as well. The FINGER command will provide you with a listing of people currently logged into the system, with some information on them, such as their full name, where their terminal is located, and what their account is known as. You will also show up on a FINGER, and it will show whether you're on a remote host or not. FINGER followed by a valid account on that system will give you some *very* detailed info on that person. One other very nice feature of FINGER is that you can supply a remote host name, and get a listing of people on another host, *without connecting to it!!* (For instance, FINGER @SRI-NIC will give you a listing of people logged onto the Network Info Center.) Another program that gives details on users (though not all that much) is SYSTAT. Both can, in many cases, be run *without logging in*, and many HELP files are also accessible without logging in. Certain HELP files give information on login formats or list dialup numbers.

If you have an account on a system, the chances are quite good that that system will support FTP, which is short for File Transfer Program. This allows you to take files from one system, and copy them to the system that you're on. The one problem here is that you will need a valid account to use on the system you wish to take the files from. Most (if not all) TOPS-20 systems support file transfers, and consequently have an account set aside for that purpose. The account is called "ANONYMOUS" and it works with any password. Some other hosts use the account "ANONYMOUS" as well, but they are by no means consistent. The way file transfers work is through an FTP on the system that you're presently on. This program communicates through ARPANet with the host you want to take files from. On the remote host, there will be a program running that will take requests from other hosts, and transmit files through the network to them. You can do more than take files, though. You can transmit files from the host you are on to the remote host, or delete or rename files on the remote host, or get a directory of an account on the remote host. It's very handy to get a file from SRI-NIC which contains all network base addresses, addresses of gateways (ways of getting from one network to another), and addresses of all hosts on all networks.

And, of course, there's the ARPANet mail system, which allows you to communicate with *any* ARPANet user. It works in a similar fashion to FTP and FINGER as far as roaming the network to find a matching username or host ID. It is still said that there is a very active hacker community living in ARPANet mailboxes and it hardly seems surprising when considering how fast and efficiently this mail system works.

The Future

Since ARPANet was designed to be, and is still being used by people who are not very familiar with computers, it will always be easy to use ARPANet, and "hop" about it. It's very unlikely that they will change it in any way, since it is, for the most part, pretty good at keeping hackers away from things that they're not supposed to be looking at.

Maybe...

Electronic Switching Advances

DESPITE OBVIOUS DRAWBACKS, ESS HAS QUITE A FEW NICE FEATURES

Although most phreaks tend to look upon Electronic Switching Systems with loathing and dread, they are admittedly fascinating animals to study. The smooth sophistication of an ESS office, small machines purring away in contrast to the deafening din of step or crossbar offices, the conspicuous *lack* of relays, the presence of *software*, the calm, controlled, atmosphere.

Horrible, isn't it? Yes, quite, but still anyone who claims to be interested in phones must learn as much as possible about ESS. So this is a rundown of some of the interesting things that ESS can do.

Here are a few things that can be done in an ESS office with individual lines that are *very difficult* to arrange in crossbar types (the phone company likes to refer to these as "classes of treatment"): **Line fixed for OUTGOING calls only.** Incoming calls are thrown to an intercept operator or recording. **Line fixed for INCOMING calls only.** Battery but no dial tone if receiver is lifted on phone. **Line fixed for outgoing LOCAL calls only.** Attempts to call the operator rejected, as are calls with zero or one as the first digit. **Line fixed for outgoing LONG DISTANCE only.** Zero or one must be first digit dialed. **Line fixed for COLLECT calling only.** Paid calls rejected, as are 3rd number or credit card billings. (Used in prisons, jails, and other controlled situations.) On these, zero is the only acceptable first digit to dial. **Line fixed for OUTGOING CALLS REQUIRE I.D.** (what used to be a "Q" number in manual handling situations) Dial your call and enter a 4-6 digit personal code. (Large companies make use of this to keep track of their employees' calls.)

It's said that there are about *fifty* classes of treatment, with class 1 being totally unrestricted (i.e. a "normal" line). As the numbers progress the types of specialties change. About 20 "classes" are available, the remaining 30 or so are merely various combinations of the first 20 (outgoing calls only *and* no long distance calls allowed, etc.). Around 85 percent of the phone lines are just your average normal arrangement—the other 15 percent are very esoteric arrangements for super-large companies, institutions, government, etc.

Some other classes of treatment that are no problem for ESS to arrange are: **Decline to accept operator assisted calls.** The operator is unable to intercept the line to test for busy or to interrupt in case of an emergency. This feature shows up a lot on modem lines, since as many have found out, an operator cutting in on data transmission will frequently wind up inadvertently disconnecting the modem. **Hotel/motel service.** A guest dials his/her calls normally, but TSPS will come on line to take the room number or credit card number *without having to dial zero plus.* TSPS sends the charges on "paid" calls back to the hotel via a private line to either a Teletype machine or billing equipment on the hotel premises. **Automatic reverse charge accepted.** This is your "800" service. Under ESS, it's possible to simply take an ordinary line (a regular seven digit phone number) and assign an "800" billing code to it. **Coin service.** This is your traditional "pay phone" but in a new arrangement. Instead of a coin hitting a lever which makes the tip go to ground for a half second (ground start line), the ESS gives "dial tone first" and instead of the five cent "ding" and the ten cent "ding ding" and the twenty five cent "dong" as the coins are deposited, the coins being deposited make certain frequencies on the line. ESS is told from a phone in this "class of treatment" to expect these frequencies, etc.

The Touchtone Problem

As most phreaks already know, if a central office is set up for touchtone service, then every line is set up for same. All one has to do to obtain touchtone service is liberate a touchtone phone someplace. If the tones don't sound when they're pressed, then the tip and ring are most likely reversed. Change the position of the red/green (yellow/black) wires and the problem should stop. But in ESS offices, you can forget it!!

In an ESS office, when you lift the receiver to make a call, you are extended one of two types of line selectors. The one is for customers who have *paid* for touchtone service. The other is for customers who are listed as having rotary service. Oddly enough, when you reverse the tip/ring, you won't get the tones—place them properly and you *will* get the tones—but—touchtones *won't cut the dial tone* in an ESS office unless you've paid for it!

This feature always causes huge problems whenever an office is cut over to ESS. For various reasons, the phone company's outside plant records are usually a complete shambles. They tend to keep very poor records about just what is on the subscribers' premises. So what usually happens is this: a big company that has their own centrex line opens its doors on Monday morning (most ESS cut-overs take place on Sunday mornings to lessen the effect of any interruption in service) and finds that half of its touchtone phones don't work! The phone company records didn't say to set up those particular lines with touchtone! Everyone has fun.

Let's Be Fair

For dedicated phreaks, ESS poses a number of serious problems. But, at the same time, an awful lot of new features (i.e. toys) are making their way in our direction, thanks to ESS. The increased ease in call supervision is one feature you don't hear much about from the phone company and one that many of us would prefer to do without. But there are these "good" things that the telco uses as a selling point in ESS—how beneficial these are to you, versus the obvious disadvantages, you'll have to decide (even though it won't change a thing).

Call Forwarding: Forward incoming calls to whatever phone you want, local or long distance. **Call Waiting:** A tone comes on the line to let you know that another call is trying to reach you while you're using the phone. **Three Way Calling:** Use the switchhook to hold one party while bringing a third party on the line. **Consultation Calling:** Like three way, but you converse privately with a third person, hang up and get the first one back who had been waiting on hold. **Speed Calling:** Allows calls anywhere in the U.S. or Canada by dialing just one digit and the star sign. **Store and Forward:** If you can't reach your party, you can dictate a voice message to the ESS computer. Tell the computer to try every fifteen minutes until the party answers, then deliver your recorded message to him. **Answering Service:** Like a phone answering machine, but it is in the computer! Dial a special code, dictate your "answering service" message and hang up. If you don't answer after a set number of rings, the computer will play your recording and take a message from the caller!

Phone companies all over are finding that these "enhanced features" are big sellers. In future issues, we'll discuss some of the bugs that have been found in these features, and in ESS systems in general.

Sophisticated as it may seem, ESS is by no means perfect.

THE DARK AND TRAGIC SIDE OF THE GREAT BREAK-UP

I have had it up to here with this divestiture crap! I consider myself to be a very loyal phone phreak who has always hated Ma Bell with a passion. What I wouldn't give to have the good old days back, when Bell was the only game in town!

Now there's this strange entity called AT&T Communications. I *still* don't know where it is they're coming from. They're not my local company. They're my long distance company that I never asked for. My local company (not AT&T!) decided to tell my long distance company that I wanted a special service that allowed me to make lots of long distance calls within my state for a discount. I didn't object at first. But then I saw myself getting charged a minimum fee every month I didn't use it! Who do I complain to? My local company? AT&T? They both blamed each other. Finally, AT&T said they'd fix it, but they never did. Now who do I complain to? The Public Service Commission in my state doesn't handle national telephone companies—only statewide ones. The business office ladies of my local company are very happy to listen to my complaints and are even happier to say, "That's AT&T, not us. We're not the same company anymore."

My local operator, for some reason, seems to be a part of AT&T. If I call to tell her that my house is burning, I fully expect to hear her say that I have to call my local telephone company and please leave AT&T out of it.

We never should have been allowed to get hooked on the Bell system—that's what spoiled us. Equal access from the beginning would have made sense. To have it suddenly start now is one big fat pain!

It's the government that's to blame, really—they're the ones that have screwed things up so badly. No one knows from one minute to the next how they're going to dial a number. First, they say we're going to dial 950-10XX for every long distance call. Then they say we're going to skip the 950 part and just dial 10XX plus the number. Now they're telling us that we're going to have to subscribe in advance to MCI, Sprint, etc. Meanwhile all of these long distance companies are popping up out of nowhere with advertising blitzes that make you feel like an idiot for not signing up right away. All it's doing is confusing the hell out of older people and people who aren't too bright as well as those who just aren't phone phreaks. My parents can't keep up from one minute to the next and I'm not much better off, despite my knowledge of the system!

The way I see it, this divestiture is going to cause all the smaller companies to give poorer service and go up on their rates even more. (Soon I won't be able to afford to call people *unless* they're long distance—local rates just keep climbing!) Local companies are letting their exchanges fall apart. They claim they're going to have to raise their rates to pay for maintaining the C.O.'s. Service has gone downhill—even worse than it ever was. The whole thing is a mess.

Think of how easy it used to be. It was you and the phone company. The phone company provided your phone, fixed your phone, gave you local calls, long distance calls, operators, free directory assistance. If you were a phone phreak, you had to worry about the phone company. Today, a phreak has to worry about so many different companies it'll make his head swim!

The old days will never come back, I guess. But let's try to remember them this way: things were horribly unfair and dictatorial. But at least everything worked. The phone company took pride in its work instead of shifting the blame to another phone company. It was easy to complain, easy to get repair service to your door, easy to figure out if you could afford to make a call. The instruments lasted forever—in fact, my phones from the forties and fifties are in *much* better shape than the new crap I have!

Today things are fair and equal, or getting there. I, for one, can really see the difference.

"LOOK OUT, HE'S GOT A COMPUTER!"

Fear of computers is one thing. Almost everyone has experienced this to some extent, though some of course are able to handle it far better than others. But *misunderstanding* of computers is a great deal more damaging and far less recognized among the mainstream.

What's the difference? The two are definitely related, there's no denying that. But they are far from identical. One of the most outstanding differences lies in the fact that people who claim to be "afraid" of computers (whether it's because of their efficiency, rapid growth, or whatever) tend to keep away from the things. But people who misunderstand computers are the ones who are running and regulating them.

Last month it was reported that Tom Tcimpidis, who operates a computer bulletin board system from his home in the Los Angeles area, had his equipment seized by the Los Angeles Police Department. Why? Somebody somewhere had called up his system and left an AT&T credit card number posted. Pacific Telephone found out and decided to flex its muscles. Officials involved in the case insist that the system operator be held responsible but it's impossible to ascertain *why*. The man who approved the search warrant, Superior Court Judge Robert Fratianne, was quoted in *InfoWorld* as saying, "As far as I can see, for someone to commit a computer crime, they have to have the knowledge, the equipment, and the access to an illegal [bulletin] board." Does anyone know what he's talking about? What in the world is an *illegal* board? What kind of equipment is he talking about? The only equipment here is a home computer! In another article, one of the officials claims that he knows all about this kind of thing, because he saw *War Games*, the film where a kid tries to start a nuclear war. Perhaps he didn't see the same film as the rest of the world, but in any event, seeing *War Games*, whether you understand it or not, doesn't make you an automatic expert on anything having to do with computers! This is what is known as aggressive ignorance.

Another fun thing that happened last month was the TRW escapade. The nation was shocked to find out that the TRW computer, which houses credit information on a *large* number of people, *might* have been broken into. Nobody knew what had even happened! Did someone raid the system and destroy or change info? Did the feds bust another BBS for posting "illegal" info? Were real criminals involved this time? Did a large bill get sent to an innocent corporation? According to all of the articles that have been written, not one of the above happened, but they all *could* have happened. So where is the story?! Are they saying that the worst thing that happened here was the posting of this nifty information somewhere? Well, that's not even interesting since any employee that uses the system could tell someone else about it at any moment.

Again, what we are seeing here is a failure to appreciate the full implications of such a thing. There is a story in this whole TRW thing. But it's not in the possibility that some hacker somewhere figured out a password. The story lies in the existence of the TRW database itself. Why was this completely downplayed? Because an article about kids breaking into a computer makes for good, sensationalist reading. It doesn't matter if most of the information is totally wrong; the people will read it. Nobody wants to read about how we're losing whatever freedom we have left, not to a machine, but to the people running the machine. It's depressing to hear about your entire life story being written to disk somewhere and to know that there's not a thing you can do about it. But, like it or not, this is *exactly* what's happening.

It's quite possible that TRW has a file on you that can be checked and appended by people all over the place. It's also entirely possible that some of that information is wrong. And it's a fact that TRW itself claims no responsibility for the accuracy of this info. But even if all of the information *is* right, how do you feel about being categorized?

In our pages, we've devoted some space to the way TRW operates and the information that can be found. We didn't print this so that everybody could figure out a way to break into their system, although we'll certainly be accused of this by our critics.

We're publishing these facts so that as many people as possible can become aware of the wide availability of increasingly personal tidbits and how this can affect us for the rest of our lives. We're doing this so that people can realize how easy it is for items to be altered and for assumptions to be made by people reading this data. Look at the sample printout and see if its thoroughness surprises you. Try to imagine how thorough it could become in ten years with improvements in technology and continued erosions of personal freedom. The FBI recently came very close to expanding its files on criminals. They wanted to include "known associates of criminals." Next would have come "known associates of known associates," etc. They lost the battle for the moment, but you can count on seeing another drive for this increased surveillance real soon.

What many are not realizing is that this constitutes true "misuse" of computers. What kind of a society are we heading towards that wants to keep close personal data on *everybody*? Regardless of whether or not one is on the right side of the law, nobody wants everything about them to be known. We all have our secrets and more systems like TRW will make those secrets increasingly hard to keep. But according to today's papers, the biggest problem with computers are the hackers.

People who do little more than type some numbers onto a terminal and do a little bit of thinking are referred to alternately as computer geniuses and computer bandits by the media. And nearly every story written about such things is full of astronomical lapses, misinformation, corporate sympathy, and the obligatory Donn Parker quotes. *The Washington Post* recently did a three-part story on "computer crime" which said absolutely nothing new. It could have been manufactured by a computer program!

Meanwhile, legislators are tripping over themselves trying to get laws passed to *control* these computer people before they take over the world. The intensity with which the FBI has chased hackers in the past year or so indicates the power they think those with computers either have or are capable of achieving. And most of this fuss is being made over people simply *accessing* other systems. What in the world is going to be the reaction when people finally start to *use* the computers, to calculate and design?

A new bill has been proposed to outlaw computer crime. Isn't that wonderful? Do you know what they consider a computer crime? Personal use of a computer in the workplace. This means that if an office worker were to open a file and write a note to himself reminding him to stop at the store later on, he'd be committing a felony. Plans are also in the works for bills that would add penalties to crimes that were committed with the help of computers. In other words, stealing is stealing, but stealing with a computer is stealing and a half.

The hysteria continues. The United States government is doing everything in its power to prevent the Soviets from obtaining computers that are practically a dime a dozen here. What good could this possibly achieve in the long run? And why pick on the computer? It's not a weapon in itself, but merely a tool. A *vital* tool, yes, but still a tool.

It's clear that computer people are in for an era of harassment from the authorities, who haven't been this riled up since Prohibition. And everyone else will be getting it from the computer abusers, who insist on tracking everything that moves. We can survive by staying awake. But we'd better start working on it.

MCI MAIL: The Adventure Continues

You really have to hand it to those folks over at MCI. First they tackle Ma Bell and now they're going after the U.S. Postal Service! MCI Mail's slogan, "The Nation's New Postal System," is printed on every bright orange envelope that they send through, you guessed it, U.S. Mail.

On this system a user is assigned a "mailbox" that he can use to send and receive mail. Sending is done either electronically, that is, to other people with MCI mailboxes or through the post office, which covers everybody else in the world. The first type of letter will cost you $1 for the first three pages while the second type is double the cost. It's also possible to send an overnight letter ($6) or a four-hour letter ($25) to some places. The purpose of MCI Mail is to stimulate the use of electronic mail by making it more accessible to the average person. For that we must give them credit — anybody can get an account on this system! There is no start-up fee and no monthly fee of any kind. To get an account, all you have to do is call them — either by voice or data. If you call by data, you'll have to enter REGISTER as the username and REGISTER as the password. The rest is self-explanatory. After a couple of weeks, you'll get in the mail (regular mail, that is) a big orange envelope that has, among other things, your password. With this info, you're now free to log onto the system, look for people you know, send and retrieve messages, read all of their help files, or even hop onto the Dow Jones News Service (watch it though — *that* can get pretty expensive!)

The system is set up on a network of Vaxes throughout the country. They've been operating since September 1983 and claim to have over 100,000 subscribers. Many of these are actually subscribers to the Dow Jones service, who are automatically given MCI Mail accounts whether they want them or not.

While the rates aren't overly expensive, they're certainly not cheap. Mailing regular letters is much cheaper and often just as fast since not every MCI Mail user checks their mailbox every day. Apart from that, though, there are many problems with the system as it stands now. For one thing, it can take forever getting on it, particularly through the 800 numbers. When you finally do get a carrier, you should get a message like this after hitting two returns:

Port 20.
Please enter your user name:

Enter the username you selected and the password they assigned you. It should say, "Connection initiated....Opened." From that point on, you're in.

But the system will often appear to be bogged down. Often you have to hit twenty returns instead of two. Sometimes the system won't let you in because all connections are "busy". Other times it will just drop the carrier. Real mailboxes don't do that.

Another thing that will drive you crazy are the menus. *Every* time you enter a command, you get a whole new menu to choose from. If you're at 300 baud, this can get pretty annoying, especially if you know what all the options are. There are two ways around this: get the advanced version, which allows you to enter multi-word commands and even store some files, at a cost of $10 per month, or simply hit a control O.

One part of the system that works fast and is very convenient is the user info. As soon as you type the command CREATE to begin writing a letter, you'll be asked who you want to send it to. Enter either the person's last name, first initial and last name, or username (which is usually one of the first two, but which can be almost anything the user desires). Immediately, you'll get a list of everyone with that name, as well as their city and state, which often don't fit properly on the line. There are no reports of any wildcards that allow you to see *everybody* at once. (The closest thing is *R, which will show all of the usernames that you're sending to.) It's also impossible for a user not to be seen if you get his name or alias right. It's a good free information retrieval system. But there's more.

MCI Mail can also be used as a free word processor of sorts. The system will allow you to enter a letter, or for that matter, a manuscript. You can then hang up and do other things, come back within 24 hours, and your words will still be there. You can conceivably list them out using your own printer on a fresh sheet of paper and send it through the mail all by yourself, thus sparing MCI Mail's laser printer the trouble. You could also share your account with somebody else and constantly leave unsent drafts for each other. Again, they have to be retrieved within 24 hours.

Yet another way of getting "free" service from these people is to obtain many different accounts. There doesn't seem to be any kind of a limit on this and since each account comes with $2 of free messages, a few accounts can get you quite a bit of free service. And, of course, there's no charge for *receiving* messages on any of these accounts.

2600 has learned of several penetrations onto MCI Mail by hackers. This isn't really surprising considering: (a) there are multiple usernames, i.e. John Smith's username would always default to JSMITH, which means that several passwords can work for one username; (b) all passwords seem to follow a similar pattern—8 characters with the odd-numbered characters always being consonants and the even-numbered ones always being vowels—any true hacker would obtain several accounts and look for any correspondence between the random password and the account number everyone is assigned; (c) MCI Mail doesn't hang up after repeated tries—the only thing that will make it disconnect intentionally is inactivity on your part.

But by far the biggest blunder that MCI Mail has made is not found on the system. It lies in their bills. *There is no carry-over from month to month!* If you get billed for $8 one month and you don't pay it, then proceed to use the system for $3 more the next month, your next bill will only show the $3! The $8 has vanished! (This is by far the dumbest mistake we have *ever* reported in these pages.)

You'll find quite a few unanswered questions in your travels through MCI Mail, which you can try to solve by reading the HELP files or by sending a *free* message to MCIHELP. It usually takes them a couple of days to respond to you instantly, however.

There are some software lapses as well. The system seems to be patterned largely after GTE Telemail, but it never really reaches that level of clarity. A small example can be seen in the scan tables, which have a heading of From, Subject, Size, etc. On outbound messages, the name of the person you're sending *to* appears under the *From* heading! Pretty silly.

MCI Mail shows every indication of overspending with a passion. Free messages, free accounts, sloppy programming, toll-free dialups, single sheets of paper (like their bills) sent in huge envelopes, etc. Either they're very optimistic out there or they're very naive.

(MCI Mail can be reached at 8004246677.)

INTRODUCING THE CLEAR BOX!

A new device has just been invented. It's called the "clear box". It can be used throughout Canada and through rural United States.

This interesting gadget works on "post-pay" payphones, in other words, those phones that don't require payment until after the connection has been established. You pick up the phone, get a dial tone, dial your number, and then put in your coins after the person answers. If you don't deposit money, you can't speak to the person at the other end, because your mouthpiece is cut off—but not your earpiece. (Yes, you can make free calls to the weather, etc. from such phones.)

In order to bypass this, all one has to do is visit a nearby electronics store, get a 4-transistor amplifier and a telephone suction cup induction pick-up. The induction pick-up would be hooked up as it normally would to record a conversation, except that it would be plugged into the *output* of the amplifier and a microphone would be hooked to the input. So when the party answers, the caller could speak through the little microphone instead. His voice would then go through the amplifier, out the induction coil, and into the back of the receiver where it would then be broadcast through the phone lines and the other party would be able to hear the caller. The clear box thus "clears" up the problem of not being heard.

The line will not cut off after a certain amount of time—it will wait forever for the coins to drop in.

Many independents are moving towards this kind of stupid payphone system. For one thing, it's a cheap way of getting DTF (dial tone first) service. It doesn't require any special equipment. That type of payphone will work on any kind of a phone line. Normally a payphone line is different, but this is just a regular phone line and it's set up so that the payphone does all of the charging, not the CO. With the recent deregulation of payphones, this kind of a system could become very popular.

TRW: Big Business is Watching You

TRW Information Services is America's largest credit reporting institute, containing the credit histories of over 90 million Americans online.

Recently it was reported that a password belonging to Sears, Roebuck, & Co. was stolen. TRW and the media are currently circulating several conflicting reports about the use of the account. Some reports insist that the account was never used illegitimately. Others say that 'criminals' used the account to pillage credit card numbers to illegally buy goods and services while knowing the account limit. Another account of the incident(s) says it was merely hackers exploring a very interesting system. It seems hard to believe that hackers managed to infiltrate TRW, since the system is basically user spiteful, but they seem to have pulled it off.

Once the subscriber initiates a connection with one of the many dial-ups, located in most major cities, the system will identify itself with TRW. It will then wait for the subscriber to send an appropriate answerback (such as a control-G). Once this has been done, the system will say CIRCUIT BUILDING IN PROGRESS along with a few numbers. After this, it clears the screen (Ctrl-L) followed by a control-Q. Once the control-Q is sent, the system is ready to accept the subscriber's request. The subscriber must first type a 4 character preamble which identifies the geographical area of the subscriber's account. For example:

TCA1 - for certain California & vicinity subscribers
TCA2 - a second TRW system in California
TNJ1 - their New Jersey database
TGA1 - their Georgia database

The subscriber then types a carriage return (followed by an optional 3 line feeds). On the next line, he must type his 3 character option. Most requests use the RTS option. OPx, RTx, and a few others exist. Some of these, such as RTA, return you with an error saying that this option is used for credit bureau collection activity only. TRW will accept an A, C, or S as the third character.

After the option (RTS), a space must be skipped, and then a 7 digit subscriber code is typed in. The first two digits represent the region in which the subscriber is located and the subscriber's industry, respectively.

Table I (first digit)

1 - TRW Eastern Region
2 - TRW Midwestern Region
3 - TRW Western Region
4 - Inquiries from Broker Customers
5 - ?
6 - Other credit reporting agencies within Eastern Region & Commercial Credit Subscribers
7 - Others within Western Region
8 - Others within Western Region

Table II (second digit)

0 - Public Record
1 - Bank
2 - Bank Credit Card
3 - Retail
4 - Credit Card
5 - Loan Finance
6 - Sales Finance
7 - Credit Union
8 - Savings & Loan
9 - Service & Professional

Using the tables above, it is evident that the stolen Sears Password from Sacramento must begin with a 33, identifying it as from the Western Region and as being a retail store.

Once the subscriber enters his 7 digit subscriber code which is printed along on the reports, he then appends a 3-4 character password immediately after it. (In the Sears example, the whole thing was: 3319122NXK. This code has allegedly been floating around hacker circles for at least two years!) Following this, he must type a space and then the full last name of the person he wants a report on. This is followed by another space and the full first name. After this comes yet another space.

Now the subscriber has 3 optional parameters. He can just type 3 periods after the first name and space or he can fill them in. The first period can be replaced by the person's middle initial, the second by the spouse's first initial, and the third by an S or a J which indicates Senior and Junior respectively.

The last of the three parameters is followed by a comma. This is immediately followed by the house number and a space. After the space, he then places the *first* letter of the street name. For example, he would type M for Main Street, a # for a P.O. box, or 3 for 32nd Street. This single character is then followed by the 5 digit zip code (mandatory) and a final comma. After the zip, he would hit carriage return and an optional line feed. (There are some special conditions which can apply to the house number—if an institution such as a school, motel, or hospital is given as the main address, 33333 would be used as the house number. When an address is General Delivery, 44444 would be the house number and G would be the street name. Others: U.S. Air Force, 55555 A; U.S. Army, 66666 A; U.S. Coast Guard, 77777 C; U.S. Marines, 88888 M; U.S. Navy, 99999 N.)

Assuming the subscriber is calling from a California business and he is requesting a report on Winston Smith at 3 Main Street, Anytown, CA 90003 he would type the following after the control-Q:

TCA2 (This identifies the subscriber as being from CA)
RTS 33xxxxxABC SMITH WINSTON ..., 3 M 90003,

In this case, the subscriber password was ABC and the account number was represented by 33xxxxx.

At this stage, he can request the report printout by typing a terminating control-S or he can tell the computer some information that it will then record into the account. This is known as using the second line, which is entirely optional. The first option that can be specified here is a previous address. This can be done by typing P- followed by the house number, a space, the first letter of the street, another space, and the full zip. For example, if Mr. Smith previously lived at 2600 Elm Street in New York City, the subscriber would type the following: P-2600 E 10001. He can then type a comma after this and move onto another option. If Mr. Smith had another previous address, the subscriber can enter it in the same fashion as above (after the comma) if he omits the P and the dash. This is followed by a comma also. He can then enter in Mr. Smith's Social Security number in the format of S-1234567890. If this is followed by a comma, he can then enter A-age or Y-year of birth (4 digits, e.g., 1984). The subscriber can next enter in information telling how much money Mr. Smith has requested and/or on what type of account. This is done by typing T- followed by a two digit account type, a 3 digit terms, and a 3 digit amount code. For instance, for a credit card account (which happens to be #18), with a limit of $100 (001), which is being financed for 24 (024) months, he would type: T-18024001. This information will show up as an inquiry under the subscriber's name on Mr. Smith's account.

There is one final option on line 2 which prints a heading at the top of the page (TRW supplies pre-printed forms with "nice" columns). If the subscriber cannot afford to buy their paper, he would probably type H-Y to get the heading. The last option on line 2 is followed by a comma, carriage return, and an optional line feed. For example:

TCA2
RTS 33xxxxxABC SMITH WINSTON ..., 3 M 90003,
P-2600 E 10001,1313 M 58102,S-1234567890,Y-1984,T-18024001,

This can then be finally entered by typing a control-S.

But wait! That's not all. The subscriber has one more option. He can specify the person's *employer*. Let's suppose that Mr. Smith works for NYTelco Security at 1095 Avenue of the Americas in New York City. The subscriber would then type:

E-NYTELCO SECURITY/1095 AVENUE OF THE AMER/ NEW YORK 10036

After this he would enter the familiar carriage return and optional line feed. (TRW emphasizes to their subscribers that this area is for the name and address of the employment only, not occupation or source of income. "Do not use terms such as 'housewife,' 'retired,' 'welfare' or 'unemployed' which could be considered damaging to the applicant," a special warning reads.) Since this is the last bit of information that the subscriber can enter, he is now forced to type the inevitable control-S.

The first line of the actual printout sends the page number, the date, the time, the port number, and the H/V (?). It will then print the person's address and their employer. After this it should print the person's actual credit history. Each individual account entry takes up 2 lines. In the first line, the account profile, subscriber's name and TRW account number, their association code, and the individual's account number with the subscriber are listed. The A on the left is the account profile. A means that the subscriber (SAKS FIFTH, as an example) transmitted this information automatically from their computer (as opposed to an M, which means that the subscriber manually

prepared forms with the info). The position of the A (or M) indicates a positive, non-rated, or negative rating (P/N) of the account. In this example, the A is under the P, therefore it reflects positively upon the account. The person has an account with Saks Fifth Avenue. Saks' subscriber number on TRW is 1347515. The person's account number with Saks is 26000000.

On the second line of each entry, the account status, date (last) reported, the date the account was opened, the type of account, the credit limit, current balance, and a credit profile are listed. For example, on the second line of the Saks entry, CURR ACCT indicates that it is a currently active revolving (REV) charge (CHG) account that was opened in October 1980. The account has a $6700 credit limit and as of April 5, 1984, the person had a $55 balance on the account. The C's and dashes indicate how the person pays the account. In March (one month prior to the balance data of 4-84), the account was paid on time. In February, two months prior to the balance date, the account was also paid on time. In January (3), the account was thirty days past due (1=30, 2=60, 3=90, etc.). In December, the account was not reported by Saks as indicated by a dash. In October, the account was sixty days past due. Court judgments, tax liens, and other interesting facts are also recorded.

The person may also have a 100 word or less statement in the file explaining certain entries in their account. (There is also another TRW service for business reports (similar to Dunn & Bradstreet) which has an entirely different set of subscriber codes and passwords, as well as access procedure.)

TRW doesn't like to be held up for anyone. Therefore, if the subscriber vegetates for more than a few seconds (i.e., he is neither sending nor receiving anything), TRW will abruptly say SERVICE INTERRUPTED; PLEASE REDIAL (EM) as it logs him off. Incidentally, any information that the subscriber types on lines 2 or 3 (i.e. age, social security number, employer, etc.) is automatically recorded on that person's file. Any previous information on the option is discarded (in most cases).

Technically, if a hacker hacked out an account belonging to a supreme court or other such institution, he could use the T-option to hack out the code for JUDGMENTS, TAX LIENS, and other neat things. He would then be able to modify anyone's account to report them bankrupt or that a judgment was handed down.

Hacking passwords is still reported to be very easy. Assuming that someone is trying to guess a password to a 3xxxxxx account, the following could be done:

TCA1
RTS 3000000AAA (return, control-S)
and the system responds with:
**** xx ** INVALID SECURITY PASSWORD**
and the hacker types:
TCA1
RTS 3000000AAB (return, control-S)
and the system responds with:
**** xx ** FORMAT ERROR**

The hacker has correctly guessed the password—it accepted the password but didn't find a name field. Since account numbers are very easy to get ahold of, the password is the only real challenge. That, and the fact that the system operates on half duplex, even parity, 7 bits, and 2 stop bits, which might catch a few by surprise.

All accounts can do reports on anyone in the United States that has a file. For example, if a California account requested data on a person in New York, the system would simply switch over to its New Jersey database to accomodate the request. A few states though, such as Tennessee, have government control over credit information. Thus, people from that state cannot be found on TRW. Can *you* be?

```
TCA2
RTS 1234567ABC SMITH WINSTON ...,3 M 90003,
P-2600 E 10001,1313 M 58102,S-1234567890,Y-1984,T-18024001,
E-NYTELCO SECURITY/1095 AVENUE OF THE AMER/NEW YORK 10036

  1  04-03-84  15:25:02   RN23  A55  SMITH                TCA1
     WINSTON SMITH                   4-84 NYTELCO SECURITY
     3 MAIN ST                            1095 AVENUE OF THE AMER
     LOS ANGELES CA 90003                 NEW YORK 10036


P / N SUBSCRIBER NAME        SUBR # ASSN          ACCOUNT #        MONTHS PRIOR
      STATUS     DATE   DATE TYPE  TERM AMT  BAL  BALANCE  AMOUNT  TO BAL DATE
      COMMENT    REP'T  OPEN                     DATE     PAST DUE 123456789012

------FILE IDENT:  SS# IS 1234567890,SPOUSE INIT IS J,YOB IS 1984

  A   B OF A                3101344 5                123426000000000
       TOO NEW RT  4-84  1-80  AUT   48 $8000 $600    4-10-84
A     S P N B                3110260 0                260000000
       CURR ACCT   10-Y  10-Y  CHG  REV  $100
A     CROCKER BANK           3120354 1                2600000000000
       CURR ACCT   4-84  5-77  C/C  REV $2000 $1219  4-17-84
A     SEARS                  3319842 0                2600000000000
       CURR ACCT   3-79  10-Y  ISC   14  $100    $0                  CCCCCCCCCCCC
A     BROADWAY               3370300 1                26000000000000
       CURR ACCT   4-84  3-83  CHG  REV $1000    $0  4-02-84         -CCCCCCCCC
A     MAY CO                 3370518 1                2600000000
       CURR ACCT   4-84  8-81  CHG  REV -$100   $28  4-16-84         CCCCC
A     BULLOCKS               3371400 1                260000000000
       CURR ACCT   3-84  1-77  CHG  REV  $300  $133  3-09-84
A     J W ROBINSONS          3371559 0                26000000
       CURR ACCT   4-84  7-82  CHG  REV  $400    $0  3-09-84         CCCCC
A     CARTE BLANCHE          3425200 1                2600000000
       CURR ACCT  12-83  5-81  CRC    1 $1400 $1484 12-31-83         CCCCCC

------*ATTN* FILE VARIATION: ZIP IS 90004/OTHER FILE IDENT: SS# IS 123333333,
            MID INIT IS Z,SPOUSE INIT IS S

A     CITIBANK               1391556 1                2600000
       CURR ACCT   2-83  6-78  CHG  REV -$100    $0  2-31-83         CCC---CCC-C
A     SAKS FIFTH             1347515 1                26000000
       CURR ACCT   4-84  10-80 CHG  REV $6700   $55  4-05-84         CC1-C2CC3CC-
A     NORDSTROM              3390206 1                26000000
       CURR ACCT   8-83  8-83  CHG  REV  UNKN    $0 12-15-83         CCCCC
A     G E C C                3600711 4                2600000000000000
       CURR ACCT  12-83  8-83  CHG  REV $1500 $1275 12-15-83
A     CRSI/DESMOND           1391554 1                260000000000000
       CURR ACCT   8-82  UNKN  CHG  REV -$100    $0                  CCC-CCCCCCCC
A     T W A                  2455618 0                2600000000
       CURR ACCT  10-Y  10-Y  CRC   24 $1500
A     SECURITY PACIFIC NATL  3110954 0                2600000000000000
       CURR ACCT  12-82  2-81  CRC  REV $2000    $0  4-09-84         CCC
A     FIRST INTERSTATE       3270827 2                26000000000000000
       CURR ACCT   4-84  6-81  CRC  REV $2500   $65  4-25-84         CCCCCCCCCCCC
A     CARTE BLANCHE          3425200 2                2600000000
       CURR ACCT  12-83  10-Y  CRC    1  $900   $97 12-31-83         CCCCCC
A     WESTERN AIRLINES       3457870 1                2600000000000000
       PAID SATIS  7-82  10-Y  CRC  REV $1200
A     FORD CRED              3620155 1                260000000000000000
       CURR ACCT  12-83  2-82  AUT   48$22200$17639 12-31-83
A     GREAT WESTERN S & L    3851009 2                26000000000
       CURR ACCT   1978  1974  R/C   30$29000
    A AFFILIATED CREDIT      3980756 0                26000000
       PD COLL AC  9-83  4-82  UNK  UNK -$100
  M   HAWTHORNE MAZDA        3967686
       INQUIRY    11-22-83
  A   MAY CO                 3370519
       INQUIRY    12-26-82     ISC
  A   B OF A                 3101344
       INQUIRY    4-22-82
A     FIRST INTERSTATE       3270827 2                26000000000000
       PAID SATIS  7-82  UNKN  CRC  REV $2000
    M CO SUP CT ANYWHERE CO  3010000 0                000000000000001
       JUDGEMENT                              $2000 STATE TAX

------END
```

BUT HOW DOES IT WORK?

How much do you really understand about the way your telephone works? Probably not as much as you should. Considering the amount of time most people spend on the contraptions, this is really quite a disgrace. Ask questions and make an effort to learn and you'll be the exception to the rule, which is basically: "Safety is Stupidity." Read on.

Wiring

Assuming a standard one-line fone, there are usually 4 wires that lead out of the fone set. These are standardly colored red, green, yellow, and black. The red and green wires are the two that are actually hooked up to your central office (CO). The yellow wire is sometimes used to ring different fones on a party line (i.e., one number, several families—found primarily in rural areas where they pay less for the service and they don't use the fone as much), otherwise the yellow is usually just ignored. On some two-line fones, the red and green wires are used for the first fone number and the yellow and black are used for the second line. In this case there must be an internal or external device that switches between the two lines and provides a hold function (such as Radio Shack's outrageously priced 2 line and hold module).

In telephony, the green and red wires are often referred to as tip (T) and ring (R), respectively. The tip is the more positive of the two wires. This naming goes back to the old operator cord boards where one of the wires was the tip of the plug and the other was the ring (of the barrel).

A rotary fone (a.k.a. dial or pulse) will work fine regardless of whether the red (or green) wire is connected to the tip (+) or ring (-). A touch-tone® fone is a different story, though. It will not work except if the tip (+) is the green wire. (Some of the more expensive DTMF fones do have a bridge rectifier which compensates for polarity reversal, however.) This is why under certain (non-digital) switching equipment you can reverse the red and green wires on a touch-tone® fone and receive free DTMF service. Even though it won't break dial tone, reversing the wires on a rotary line on a digital switch will cause the tones to be generated.

Voltages, Etc.

When your telephone is on-hook (i.e., hung up) there are approximately 48 volts of DC potential across the tip and ring. When the handset of a fone is lifted, a few switches close which cause a loop to be connected (known as the "local loop") between your fone and the CO. Once this happens, DC current is able to flow through the fone with less resistance. This causes a relay to energize which causes other CO equipment to realize that you want service. Eventually, you should end up with a dial tone. This also causes the 48 VDC to drop down into the vicinity of 12 volts. The resistance of the loop also drops below the 2500 ohm level, though FCC licensed telephone equipment must have an off-hook impedance of 600 ohms.

As of now, you are probably saying to yourself that this is all nice and technical but what the hell good is the information. Well, also consider that this drop in impedance is how the CO detects that a fone was taken off hook (picked up). In this way, they know when to start billing the calling number. Now what do you suppose would happen if a device such as a resistor or a zener diode was placed on the *called* party's line so that the voltage would drop just enough to allow talking but not enough to start billing? First off, the calling party would not be billed for the call but conversation could be pursued. Secondly, the CO equipment would think that the fone just kept on ringing. The Telco calls this a "no-no" (toll fraud to be more specific) while phone phreaks affectionately call this mute a black box.

How These Boxes Are Built

It's really surprisingly easy to build a device such as a black box. If it weren't for the amazingly high morals inherent in today's society, you'd most certainly see more of them in use. Only two parts are needed: an SPST toggle switch and a 10,000 ohm (10 K), ½ watt resistor. Any electronics store should stock these parts.

A person would then cut 2 pieces of wire (about 6 inches long) and attach one end of each wire to one of the terminals on the switch. Then the K500 (standard desk fone) would be turned upside down and the cover taken off. A wire would be located and disconnected from its terminal. The switch would then be brought out the rear of the fone and the cover replaced. Labelling the switch usually comes next. A position where one receives a dial tone when picking up is marked "NORMAL". The other side is, naturally, "FREE".

Making Them Work

When phriends call (usually at a prearranged time), the person with the black box quickly lifts and drops the receiver as fast as possible. This stops the ringing (if not it must be done again) without starting the billing. This must be done within less than one second. The phone can then be picked up with the switch in the "FREE" position. Most phone phreaks are wise enough to keep their calls under 15 minutes in length, greatly minimizing the odds of getting caught.

Some interesting points: (1) If someone picks up an extension in the called party's house and that fone is not set for "FREE", then billing will start. (2) An old way of signalling a phriend that you want to call him is to make a collect call to a non-existent person in the house. Since the phriend will (hopefully) not accept the charges, he will know that you are about to call and thus prepare the black box (or vice versa). (3) The phone company can detect black boxes if they suspect one on the line. This is done due to the presence of AC voice signal at the wrong DC level! (4) The black box will not work under ESS or other similar digital switches since ESS does not connect the voice circuits until the fone is picked up (and billing starts). Instead, ESS uses an "artificial" computer generated ring.

Ringing

To inform a subscriber of an incoming call, the telco sends 90 volts (PK) of pulsing DC down the line (at around 15 to 60 Hz; usually 20 Hz). In most fones this causes a metal armature to be attracted alternately between two electro-magnets thus striking 2 bells. Of course, the standard bell (patented in 1878 by Tom A. Watson) can be replaced by a more modern electronic bell or signalling device.

Also, you can have lights and other similar devices in lieu of (or in conjunction with) the bell. A simple neon light (with its corresponding resistor) can simply be connected between the red and green wires (usually L1 and L2 on the network box) so that it lights up on incoming calls.

Be advised that 90 VDC can give quite a shock. Exercise extreme caution if you wish to further pursue these topics.

Also included in the ringing circuit is a capacitor to prevent the DC current from interfering with the bell (a capacitor will pass AC and pulsing DC while it will prevent straight DC from flowing—by storing it).

Another reason that telcos hate black boxes is because ringing uses a lot of common-control equipment in the CO, which use a lot of electricity. Thus the ringing generators are being tied up while a free call is being made. Usually calls that are allowed to "ring" for a long period of time will be construed as suspicious. Some offices may be set up to drop a trouble card for long periods of ringing and then a "no-no" detection device may be placed on the line.

Incidentally, the term "ring trip" refers to the CO process involved to stop the AC ringing signal when the calling fone goes off hook.

It is suggested that you actually dissect fones to help you better understand them (regardless of whether or not you want to build any devices). It will also help you to better understand the concepts here if you actually prove them to yourself. For example, actually take the voltage readings on your fone line (any simple multi-tester (a must) will do). Phreaking and/or learning is an interactive process, not a passive one!

(Any questions on the above? Write us and we'll try to answer them.)

PRIVACY LOST

The Rise of the Computer State
by David Burnham
w/foreword by Walter Cronkite
Vantage Books $6.95 paperback 273 pp.

Several years ago on *Sixty Minutes*, a segment was presented where all of the checks that one person had written in his lifetime were examined, and then a fairly accurate portrait of the person's life was painted by the discrete bits of information. Information like this is called transactional information and we leave huge amounts of it behind as we live our lives, whether in tons of paper or megabytes of data.

In *The Rise of the Computer State*, David Burnham says that an event as demonstrated by the *Sixty Minutes* team could happen and many similar ones do occur. He surveys many of the ways that computers and technology can be used to intrude upon our privacy; the governmental mandates for such intrusion; and how, in general, computer abuses have affected history.

Burnham begins with a review of computer history and the importance of computers on our lives. While always implying a global connection, he concentrates upon the United States where "industries engaged in the processing of information... now generate about half the GNP." Later Burnham brings up legal points which are supported by examples. He also discusses legislative battles and presidential directives both for and against the public good. Overall, *The Rise of the Computer State* reveals in technical and ethical terms how close we are to Orwell's technocracy.

Christopher Evans, a psychologist and computer scientist said that if during the 30 years from 1945 to 1975, the automobile had developed as fast as the computer, the Rolls Royce would cost $2.75, would have enough power to push the Q.E. II across the Atlantic, and would get 3 million miles to the gallon.

The computer has that amazing ability to quickly and efficiently move and sort through vast amounts of information, and this is why they are being used in all aspects of society including the FBI, police, banks, phone companies, and credit companies. They are used by most businesses for payroll, personnel, inventory, accounting. They are used by most government agencies including the IRS, FBI, CIA, SSA, NSA, HEW, FRB, and a large number of others. In fact, he devotes an entire interesting chapter on the National Security Agency (NSA) which was obviously written before *The Puzzle Palace*, a rather thorough examination of the NSA, was published. (A future issue of *2600* will look at the NSA.)

Computers are used to compile lists, store data, pay employees, transfer funds, make airplane reservations or phone calls, communicate, write letters, address envelopes, detect incoming ICBM's, price goods at supermarkets and department stores, tell time, and keep track of America's airplanes and trains to prevent them from crashing. There are literally millions of things computers can do to benefit humankind.

But the most amazing of these computers are controlled by big government or a few corporations. Transactional information about our lives is often bought and sold and traded without our permission. In bank computers lie copies of the checks we wrote. In our hospital computers are our medical records. In many states, computer files are kept on all prescriptive medicine. In many law enforcement computers lie arrest and conviction records, often incomplete or inaccurate as Burnham points out.

- Our movements can be kept track of by looking at our phone charges, airline, bus, train, and car rental records, or our gas receipts.
- In Pittsfield, Mass., people's buying habits are computerized and compared to the special dose of commercials that are sent to only their television sets. If we get supermarket credit cards, then every item, all of our individual buying habits, can be examined.
- Information from the 1940 census was used to round up Japanese into concentration camps. If another thoughtless government wanted to do something again, it won't be hard.
- In Los Angeles there is a registry of "undesirable" tenants that can be accessed for a fee. The information is often just heresay or the opinion of a past landlord. If the information is negative, the potential tenant is turned down.
- The FBI possesses the fingerprints of 66 million people in its criminal or civil identification files.

Burnham brings up the topic of criminal records a lot—about how past arrests and convictions can follow a person, even if a case is dismissed. This information is available to law enforcement agencies, government personnel departments, and private companies. These databases of criminal records, which only one out of every five states have ever checked for accuracy, were created in order to apprehend criminals. But if these records are used to keep suspected criminals or ex-cons out of governmental and private jobs and thus keep them unemployed, these people are practically forced to return to crime.

By cross matching files, politicians can locate key groups to appeal to in order to make decisions or win elections. By cross matching files, likely suspected communists can be systematically tortured, or customers for a new store can get junk mail designed just for them. In the can-anything-be-done chapter, we are left to hope that some laws or presidential orders are created to stop cross matching of information between government agencies. There are examples where things are done (and undone again) in an effort to preserve privacy, but as we see much information about us is public. Until recently, the selective service was aware of who got free ice cream from Farrow's. It won't be long until all of the Flintstone vitamin peddlers will be buying up the list of the cabbage patch parents from Coleco. Companies are always buying information about us to gain an economic advantage. Business controls money and hence information. This information gives them direct power and often a marketable item. TRW and other lesser known credit companies sell information to other businesses for about a buck a report, but to check your own record in order to see if the report is accurate costs $12. Mailing lists pass hands like stocks on Wall Street.

But are we threatened now? When it comes to criminal records, IRS, and credit stuff the info is being used widely. The federal government is tightening up on documents it makes public. But often Mr. Burnham is telling us what is possible which is not far from the actual. He doesn't stress the importance that the Freedom of Information Act had which is being gutted by the Reagan Administration.

What Mr. Burnham could have done to make his case even more effective is to include actual examples of the vast personal data and create a small autobiography based on his own credit history, bank records, FBI files, criminal records, motor vehicle records, college records, and other similar sources. He could have gotten some experts to examine all of his transactional information and then compare it to himself. But it's all right for Burnham not to do this, because he suggests to us that such a thing can be done.

Burnham goes on and on citing legal abuses, privacy intrusions, and political and economic manipulation. The book reads like those old TRW ads: "Imagine a day when..." and it ends the same way: "... That day is today. Write to us—we'll tell you all about it." Burnham tells us almost all about "it" too. He does not mention the danger to a computer state where a disgruntled employee or little kiddie at a terminal can crash a huge system permanently, or a clever sadist can create a viral program that can spread throughout a database and wipe out file after file! Burnham does not mention the technological pioneers who hack and explore and understand the world that is approaching and encroaching and who warn others of the danger. Mr. Burnham would appreciate the work of some of the people like that, just as we can appreciate the warnings in his book about the power of the technological elite.

The Rise of the Computer State represents one of the many books that should be read to prepare for the future as well as the present. Mr. Burnham has managed to condense an immense amount of information on the power and threat of computers and data collecting agencies. His book is well researched, but he needs that extra something to retain the sympathy of those who have "nothing to hide" and the interest of those who cannot relate to terms like "dehumanization" and "values". *The Rise of the Computer State* startles one with a slap of hidden reality, and this is what we need now.

BE NICE TO YOUR TELCO

Over the years, some bad things have happened to my telephone. Once a silly caller terminated his call but did not hang up. I called the phone company (New York Telephone) from a neighbor's phone, but they said they were unable to do anything. They said they could not even tell me where the caller's phone was located. Acting on a hunch, I cruised my neighborhood looking for pay-phones. I found the phone I was interested in, but it was in a locked building, and I clearly saw the receiver dangling. The next morning I was able to hang up the phone, and my phone service was back to normal.

Another time the clever sewer workers hauled out my trunk and knocked out my phone. It was restored, but I was not getting any incoming service after that. The even more clever phone man came over, dialed the Automatic Number Identification, and lo and behold I had a new number. They fixed that too.

My phone company has been generally nice to me even though I played some jokes on them. I suggest you do not do the following, as I have done in the past:

- Fold, spindle, and mutilate your billing card.
- Punch extra holes in it to increase your bill $10,000 or more.
- Cross out the line of numbers in magnetic ink at the bottom of your bill or check.
- Make out your check to a penny less or a penny more than what is due.
- Order as many free phone books for as many areas as possible.
- Order phone books for obscure areas covered by private phone companies.
- When you have free checking, pay with more than one check (10 or 20 per phone bill, for example).
- Write with thick black marker the word **FUCK** at the bottom of your check where the space for memos is located.

These activities cause the phone company to put more work into serving you. It causes them to process your bill by *hand*, to spend money printing and mailing phone books, and to read your unfriendly message. Don't do this or your rates will go up. *(Please contact 2600 IMMEDIATELY if you know of other abuses currently making the rounds.)*

HISTORY OF BRITISH PHREAKING

by Lex Luthor and The Legion of Doom

In Britain, phreaking goes back to the early fifties, when the technique of "Toll A drop back" was discovered. Toll A was an exchange near St. Pauls which routed calls between London and the nearby non-London exchanges. The trick was to dial an unallocated number, and then depress the receiver—rest for ½ second. This flashing initiated the "clear forward" signal, leaving the caller with an open line into the Toll A exchange. He could then dial 018, which forwarded him to the trunk exchange—at that time, the first long distance exchange in Britain—and follow it with the code for the distant exchange to which he would be connected at no extra charge.

The signals needed to control the UK network were published in the *Institution of Post Office Engineers Journal* and reprinted in the *Sunday Times* 15 Oct. 1972. (NOTE: The British Post Office is the U.K. equivalent of Ma Bell.)

The system is called Signalling System No. 3 and it uses pairs of frequencies selected from 6 tones separated by 120Hz. With that info, the phreaks made "Bleepers" or as they are called here in the U.S., blue boxes. The British, though, utilize different MF tones than the U.S., thus, your U.S. blue box that you smuggled into the U.K. will not work, unless you change the frequencies. (In the early seventies, a simpler system based on different numbers of pulses with the same frequency (2280Hz) was used. For more info on that, try to get ahold of: Atkinson's "Telephony and Systems Technology".

Boxing in Foreign Lands

The following are timing and the frequencies for boxing in the U.K. and other foreign countries. Special thanks to Peter McIvers for the following info:

British "bleeper" boxes have the very same layout as U.S. blue boxes. The frequencies are different, though. They use two sets of frequencies: forward and backward. Forward signals are sent out by the bleeper box. The backward signals may be ignored (it's sort of like using full duplex). The frequencies are as follows:

U.S.	700	900	1100	1300	1500	1700 Hz
Fwd	1380	1500	1620	1740	1860	1980 Hz
Bkwd	1140	1020	900	780	660	540 Hz

For example, change the 900Hz potentiometers in your box to 1500Hz. All numbers 1-0 (10) are in the same order as in an American box. The ones after this are their codes for operator 11, operator 12, spare 13, spare 14, and 15. One of these is KP, one (probably 15) is Star; it won't be too hard to figure out. The signals should carry -11.5dBm +/- 1dB onto the line; the frequencies should be within +/-4Hz (as is the British equipment). Also, the 1VF system is still in operation in parts of the U.K. This would encode all signals 1 to 16 as binary numbers; for instance, a five is 0101. There are six intervals per digit, each 50ms long or a total of 300ms. First is a start pulse of 2280 for 50ms. Then, using the example of five (0101), there is a 50ms pause, a 50ms pulse of 2280, a 50ms pause, and a 50ms pulse of 2280. Finally, there is a 50ms pause that signals the end of the digit. The frequency tolerance on the 2280Hz is +/-0.3%; it is sent at -6 +/- 1dBm. An idle line is signalled by the presence of a 3825Hz tone for more than 650ms. This must be within 4Hz.

France uses the same box codes as the U.S., with an additional 1900Hz acknowledgement signal, at -8.7 +/- 1dBm per frequency.

Spain uses a 2 out of 5 mf code (same frequencies as U.S.), with a 1700Hz acknowledge signal.

Other places using the 1VF system are:

Australia: 2280Hz +/-6Hz, 35ms/digit at -6dB.

Germany, France: same as Australia; also, some 1VF systems in the UK.

Switzerland: same as Australia, only it uses 3000Hz, not 2280.

Sweden: same as above, but at 2400Hz.

Spain: some parts use 1VF with 2500Hz.

There is one other major system: the 2VF system. In this system, each digit is 35ms long. The number is encoded in binary as with the 1VF system. Using the example of five (0101), here's how the American 2VF system was sent:

2400 pulse, pause, 2040 pulse, pause, 2400 pulse, pause, 2040 pulse, pause. The digits and pulses are all 35ms long for a total of 280ms per digit.

Other countries are still using a similar high/low pair with the same timings. Some parts of **Italy** use the 1VF system with 2040Hz; some use the 2VF system with 2040 and 2400Hz (same as original U.S.). **The Netherlands** uses a 2VF system with 2400 and 2500Hz pulses. With the 2VF system, all frequencies should be within 2Hz.

Also, here are some specs for American phone equipment:

Dial Tone: 350+440Hz, -17.5 to -14.5 dBm/tone,

Off-Hook (ROH): 1400+2060+2450+2600(!) on/off 5 times per second.

Busy: 480+620Hz; slow busy: 0.5 +/- 0.05 sec = 1 period (about twice a second), at -28.5 to -22.5 dBm/tone.

Ring: 440+480Hz at -23.5 to -20.5 dBm/tone. A ring is modulated at 20 +/-3Hz, 2 sec on, 4 sec off.

Call Waiting: 440Hz, on 1 second.

Recorder Connection: 1400Hz, beeps every 15 seconds.

Multiparty Line Ring: same frequency and modulation as ring, but 1 sec on, 2 sec off (twice as fast).

Titan the Scanner

In the early days of British phreaking, the Cambridge University Titan computer was used to record and circulate numbers found by the exhaustive dialing of local networks. These numbers were used to create a chain of links from local exchange to local exchange across the country, bypassing the trunk circuits. Because the internal routing codes in the U.K. network are not the same as those dialed by the caller, the phreaks had to discover them by "probe and listen" techniques, more commonly known in the U.S. as scanning. What they did was put in likely signals and listen to find out if they succeeded. The results of scanning were circulated to other phreaks. Discovering each other took time at first, but eventually the phreaks became organized. The "TAP" of Britain was called "Undercurrents" which enable British phreaks to share the info on new numbers, equipment, etc.

To understand what the British phreaks did, think of the phone network in three layers of lines: local, trunk, and international. In the U.K., Subscriber Trunk Dialing (STD), is the mechanism which takes a call from the local lines and (legitimately) elevates it to a trunk or international level. The U.K. phreaks figured that a call at trunk level can be routed through any number of exchanges, provided that the right routing codes were found and used correctly. They also had to discover how to get from local to trunk level either without being charged (which they did with a bleeper box) or without using (STD). Chaining has already been mentioned but it requires long strings of digits and speech gets more and more faint as the chain grows, just like it does when you stack trunks back and forth across the U.S. The way the security reps snagged the phreaks was to put a simple "printermeter" or pen register, as we call it, on the suspect's line, which shows *every digit dialed* from the subscriber's line.

The British prefer to get onto the trunks rather than chaining. One way was to discover where local calls use the trunks between neighboring exchanges, start a call, and stay on the trunk instead of returning to the local level on reaching the distant switch. This again required exhaustive dialing and made more work for Titan; it also revealed "fiddles", which were inserted by Post Office Engineers. What fiddling means is that the engineers rewired the exchanges for their own benefit. The equipment is modified to give access to a trunk without being charged, an operation which is pretty easy in Step by Step (SxS) electromechanical exchanges, which were installed in Britain even in the 1970's.

A famous British "fiddler" revealed in the early 1970's worked by dialing 173. The caller then added the trunk code of 1 and the subscriber's local number. At that time, most engineering test services began with 17X, so the engineers could hide their fiddles in the nest of service wires. When security reps started searching, the fiddles were concealed by tones signalling: "number unobtainable" or "equipment engaged" which switched off after a delay. The necessary relays are small and easily hidden.

There was another side to phreaking in the U.K. in the sixties. Before STD was widespread, many "ordinary" people were driven to occasional phreaking from sheer frustration at the inefficient operator controlled trunk system. This came to a head during a strike about 1961 when operators could not be reached. Nothing complicated was needed. Many operators had been in the habit of repeating the codes as they dialed the requested numbers so people soon learned the numbers they called frequently. The only "trick" was to know which exchanges could be dialed through to pass on the trunk number. Callers also needed a pretty quiet place to do it, since timing relative to clicks was important.

The most famous trial of British phreaks was called the Old Baily trial which started on 3 Oct. 1973. What the phreaks did was dial a spare number at a local call rate but involving a trunk to another exchange. Then they sent a "clear forward" to their local exchange, indicating to it that the call was finished—but the distant exchange didn't realize this because the caller's phone was still off the hook. They now had an open line into the distant trunk exchange and they sent a "seize" signal (1) which put them on the outgoing lines. Since they figured out the codes, the world was open to them. All other exchanges trusted the local exchange to handle the billing—they just interpreted the tones they heard. Meanwhile, the local exchange collected only for a local call. The investigators discovered the phreaks holding a conference somewhere in England surrounded by various phone equipment and bleeper boxes, also printouts listing "secret" Post Office codes. The judge said, "Some take to heroin, some take to telephones." For them phone phreaking was not a crime but a hobby to be shared with phellow enthusiasts and discussed with the Post Office openly over dinner and by mail. Their approach and attitude to the world's largest computer, the global telephone system, was that of scientists conducting experiments or programmers and engineers testing programs and systems. The judge appeared to agree, and even asked them for phreaking codes to use from his local exchange!

MORE ON TRASHING

What to look for, how to act, where to go

by The Kid & Co. and The Shadow

An inspection of your local Telco office trash receptacles can reveal a wealth of documents of great interest to a telecommunications hobbiest. The fone company doesn't expect anyone except maybe bums to paw through their refuse, and therefore often disposes some interesting materials. In all the installations we have investigated, the Company doesn't shred or incinerate anything. Most sites have their garbage in trash bags convenient for removal and leisurely inspection at home.

A case in point. The authors of this article have been engaged in trashing for about three months, finding quite informative info, but when we escorted two phriends from the city on an expedition, we didn't know the most efficient methods. They came out to the boondocks of New Jersey to inspect the wealth of AT&T and Bell installations in the region. They were quite expert at trashing, having more experience in the art, so we merely watched and copied their technique.

Our first hit of the night was of an AT&T Information Systems office building. We gathered a large mass of manuals and binders. Then we moved onward to hit AT&T Communications, the local business office, our central office, and another Bell site. After a successful session, we decided to call it a night.

We sorted the piles of garbage for things of merit. Our phriends garnered the majority of the really interesting items, but we salvaged several things of worth. This sorting session was conducted in the center of town, to the amusement of passers-by. It was interesting to explain to friends that passed by what we were doing. We BS'ed an inquisitive young lady into thinking that we were a local group of Boy Scouts cleaning the area as a project for our Eagle Scout badge. Following the tendency of the masses to follow falsehoods, she complimented us on how clean the town looked, for she had been out of the country for the last couple of months. Just remember when "creatively explaining" to sound confident, and to have your compatriots shut their mouths. A couple of times we almost contradicted each other as everyone got into the flow of falsehoods.

Numerous things of interest can be found in Bell trash. Ones that are of use to anyone are binders and notebooks with the Bell logo on them, good for impressing friends. Also, supplies of Bell letterhead are good for scaring phriends. Documents of more interest to phreaks can also be found. Cosmos printouts abound in any CO trash. In house telephone directories list employees of Bell, good to try social engineering on. Manuals also have merit for the phreak. Maintenance reports, trunk outages reports, line reports, network control analysis (NCA), TSPS documents, and lists of abbreviations used by the fone company can be found. The latter is of great importance as it allows one to decipher the cryptic documents. Bell seems to love ridiculous and mysterious abbreviations and anacronyms.

"Looking for Notebooks"

The expert trasher must be willing to physically enter the dumpster. Only reaching in for easily obtainable objects misses heavy manuals that tend to sink to the bottom. Huge bulky printouts, directories, and obese manuals as well as binders settle out of reach. Also, once in the dumpster, inquisitive security can't see you.

Speaking of security, what are the dangers of trashing? Well, we don't know, having never been caught at it. The basic fact which protects the trasher is the ludicrousness of someone stealing your garbage. Probably the most they can get you for is trespassing, and most of the time they'll probably just throw you off the property. Good excuses for being around the dumpsters are that you are passing through on a shortcut, that a ball or frisbee has flown in, or that you are looking for notebooks for school.

A good way to avoid unnecessary surveillance by Telco employees is to trash late at night, after most have gone home. Weekends, especially Sunday nights, leave the sites deserted, except for security or janitorial staff. Before starting on a trashing run, be sure to reconnoiter the area, and to find out the schedule of garbage collection. That way you can hit the trash at the fullest and most profitable time.

One thing that simplifies trashing runs is the use of a car. A car will allow one to hit trash sites farther afield, as well as assisting in the removal of bags and boxes of trash to sort at your leisure. Trash sorting really shouldn't be done on site as it increases the possible time for discovery by security. Removing garbage by foot invites stares and limits the amount that can be removed. The car should drop off the trashers and return about a half hour later, depending on the amount of trash there. Before dropping them off, be sure to investigate if there is any trash in the first place for, as past experience has shown, they tend to get quite angered when they have spent the last hour staring at an empty trash container.

The on-site trashers should be willing to hop into the dumpster. As we mentioned, this maximizes the amount of trash that can be reached. They should rip open any bags, shoving the uninteresting ones to the rear and bottom of the container, while bringing new ones to the forefront. Boxes in the trash should be used to carry the documents into the trunk of the car for leisurely sorting. This should be done with a minimum of noise and light, if flashlights are to be used. The trashers shouldn't attempt to take the best stuff, just to grab as much as looks interesting.

At the appointed time, the car should return and pick up the trashers. Boxes should be stuffed in the trunk as quickly as possible. Smell won't be much of a problem, as all you are taking are papers. Occasionally a bag of coffee grinds smells up the works, but you, at all costs, should avoid cafeteria dumpsters as the rotting food really reeks, and contains little of value to the telecommunications hobbiest.

The car should then drive off to a safe and secluded spot to sort the trash. The location should be well lit and have another dumpster handy to throw the real trash out permanently. The valuable stuff should be taken home and sorted according to type. By keeping all of the similar stuff together, patterns can be recognized. Here, abbreviation lists come in handy. The date and location where the trash is located helps to keep the junk organized.

A careful inspection of local Telco trash receptacles can be informative and fun. Any real phreak should find out at the least what the switching equipment for his/her/its area is. Proper trashing technique is gained by experience, so climb on in! Well, happy trashing and have a phree day.

A FRIEND IN HIGH PLACES
YET ANOTHER TRUE STORY OF TELECOMMUNICATION FUN

Once upon a time there was a most unusual phone phreak and it was a phone phreak who didn't realize it. Her name was Joanne. She had a very remarkable position in that she was a telephone operator in an extremely small, rural, midwestern community. A friend of mine, who was a radio D.J., got a job in this small town. One night he had a few drinks after he got off work. He called this operator up and started talking to her for a while. She didn't hang up. In fact, she was quite cordial, quite nice, quite friendly. She said, "Would you like to call Dial-a-Record (in Australia)? Or Dial-the-Time in London? Or any other dial-it services? If there are any phone calls you'd like me to place *for free*, just let me know."

So Joanne proceeded to place a lot of long distance calls for the guy for free. He introduced me to her and said you can call Joanne for free by dialing a certain out-of-service number. She'd say, "What number did you dial, please?" And then she would quickly forward it to the other intercept operator in the nearby large city where she would tell the operator what number was dialed and then they'd put on the standard out-of-service or number-changed recording. I'd say, "Hey Joanne, it's me, call me back!" And she would. And I'd talk to her all night long because I was a security guard at the time. We'd place long distance calls, conference calls like you wouldn't believe. One day she said that the switchboard was going to get phased out—a new TSPS switchboard was being installed in the large community and was going to serve all of the small communities in a four or five state area.

But Joanne continued to be a phone phreak and to this day she's working as a secretary for a senator in Washington, DC. She still does some pretty remarkable things, even though she's not an operator.

You might want to call up your local operator, provided you live in a small town, and just say hi sometime. I've done it on occasion and operators are usually fairly friendly, but far from phone phreaks. You might want to try this with directory assistance (they double as operators in smaller locales).

Who knows, you might find another Joanne someplace. One never knows.

getting caught: hacker's view

Deep down, every hacker wants to get caught. Computer hacking isn't really the same as killing or stealing, after all. You need at least a *little* brains to be able to hop around on the corporations' DECsystems or to know the ARPANet better than your own PC. So if and when you get caught, you wind up getting a little bit of credit for having some brains. Most people exaggerate and call you a genius! Who can resist *this* type of an ego boost?

So when the FBI came knocking at my door early this spring, it seemed like the beginning of an adventure. It was *me* they were after! I had done something to deserve national attention!!

At first I didn't know what it was they wanted. They came to my house before I was awake and showed my mother the search warrant. I'll never forget the tone in her voice when she called me that day. "You'd better come down here right away," she said, sounding very worried and pissed off at the same time. I knew something was up when I heard that.

So then I came downstairs and saw what was happening. I was very calm throughout the whole thing—I even kept my sense of humor. After I figured out which of my many "projects" they were interested in, I showed them where all the good stuff was hidden. "Go tell the world," I said.

I had been hacking for about a year. I seemed to pick up things incredibly fast and before I knew it, I was buried inside the weird world of phones and computers. In this case, I had been running a huge corporation's mainframe for them for a few months. This computer had so much data in it that I could find out (and change) just about anything—paychecks, profit margins, telephone numbers, you name it. I had lots of fun.

My friends used to come over late at night and watch me explore. Nobody they knew had ever been able to do anything like that and it seemed pretty amazing. Then *War Games* came out and I turned into a sort of cult figure in my neighborhood. But it was OK—nobody knew *exactly* what I was doing.

Even my parents didn't seem to mind that much. They'd shake their heads and wonder what kind of mischief I'd get into next. Most people (grown-ups, that is) seemed to act exactly the same. And my friends were all into it as something fun and rebellious.

So now that I was caught, I expected the fun to continue. My parents would be outraged that a mischievous kid was being hounded by the feds while murderers and presidents were roaming free. And of course, my friends would stick by me more than ever. We were pretty tight.

For about a day, that's exactly what happened. My name got in all the papers, I was on a few news shows, and nobody really understood anything. I suddenly became popular at school. Everybody seemed to agree that it wasn't fair for them to come to my house and take away my two computers just like that.

Then, after the initial shock, people's moods started to change. My parents were the first. They suddenly got mad at me. "What a stupid thing to do!" I remember those words. "If you don't care about yourself, at least think about what you're doing to your family," and so on. They also said that I never listened when they told me to knock it off, which was totally false, since they never really seemed to care at all.

But all that didn't upset me. After all, parents are supposed to say those kinds of things. I knew they really cared, so it didn't matter what they said.

It wasn't until a few more weeks that the really bad stuff started happening. The feds began calling my friends and tried to scare them into saying incriminating things about me. They told them they'd be in just as much trouble if they didn't say anything. I could tell something was wrong when all of a sudden no one was talking to me. People I used to hang out with suddenly seemed uneasy when I was around.

Then the feds started calling *me*. And I could tell from the pointed questions they were asking, that someone I trusted had told them a lot. Much more than they had to. It wasn't like they had just cracked and said, yes, he did this and that. They *volunteered* information!

I tried to figure out why someone would do this—no one I knew had any grudges against me. I didn't really have any enemies. They must have thought that telling everything was for my own good. The feds had probably told them that I was really sick and needed help and that only the truth would set me free. Could that have been it?

It might have been. But there was definitely more than that. When the feds started scaring my friends, that was my fault. At least it seemed that way to my friends. A couple of them got so scared that their families hired these big, expensive lawyers. And that was my fault, too, even though I knew they were being ripped off.

So what did I get out of the whole thing? Well, nobody trusts me anymore—people are even afraid to let me use their phone. I've gotten a reputation as someone who doesn't care at all about his friends, otherwise how could I have put them in such a spot? Everyone in town knows that I did something bad to some corporation somewhere, but nobody understands how much of a game the whole thing seemed at the time. The newspapers were never really interested in my side and nobody else seems to be either.

Maybe this is good in a way, because I found out that most people value friendship less than their own safety. As soon as the pressure is applied, they lose all feeling for you. Then they trick themselves into believing that you were always a bad seed from the start. They do this so they won't feel guilty about the way they shafted you. But there were a couple of others who didn't desert me because they knew who I really was. If it wasn't for them, I might have just jumped off a building one night. That's how bad it makes you feel sometimes.

Yes, I'm through hacking. Let the professionals do it—they can't get hurt like I was.

Name withheld by request.

VITAL INGREDIENTS

SWITCHING CENTERS AND OPERATORS

Every switching office in North America (the NPA system) is assigned an office name and class. There are five classes of offices numbered 1 through 5. Your CO is most likely a class 5 or end office. All Long-Distance (Toll) calls are switched by a toll office which can be a class 4, 3, 2, or 1 office. There is also a 4X office called an intermediate point. The 4X office is a digital one that can have an unattended exchange attached to it (known as a Remote Switching Unit—RSU).

The following chart will list the office number, name, and how many of those offices existed in North America in 1981.

Class	Name	Abb.	# Existing
1	Regional Center	RC	12
2	Sectional Center	SC	67
3	Primary Center	PC	230
4	Toll Center	TC	1,300
4P	Toll Point	TP	
4X	Intermediate Point	IP	
5	End Office	EO	19,000
R	RSU	RSU	

When connecting a call from one party to another, the switching equipment usually tries to find the shortest route between the Class 5 end office of the caller and the Class 5 end office of the called party. If no inter-office trunks exist between the two parties, it will then move up to the next highest office for servicing (Class 4). If the Class 4 office cannot handle the call by sending it to another Class 4 or 5 office, it will be sent to the next office in the hierarchy (3). The switching equipment first uses the high-usage interoffice trunk groups. If they are busy it goes to the final trunk groups on the next highest level. If the call cannot be connected then, you will probably get a reorder [120 IPM (Interruptions Per Minute) signal—also known as a fast busy]. At this time, the guys at Network Operations are probably going berserk trying to avoid the dreaded Network Dreadlock (as seen on TV!).

It is also interesting to note that 9 connections in tandem is called ring-around-the-rosy and it has never occurred in telephone history. This would cause an endless loop connection (an interesting way to really screw up the Network).

The 10 regional centers in the United States and the 2 in Canada are all interconnected. They form the foundation of the entire telephone network. Since there are only 12 of them, they are listed below:

Class 1 Regional Office Location	NPA
Dallas 4 ESS	214
Wayne, PA	215
Denver 4T	303
Regina No. 2 SP1-4W [Canada]	306
St. Louis 4T	314
Rockdale, GA	404
Pittsburgh 4E	412
Montreal No. 1 4AETS [Canada]	504
Norwich, NY	607
San Bernardino, CA	714
Norway, IL	815
White Plains 4T, NY	914

In the Network, there are three major types of switching equipment. They are known as: Step, Crossbar, and ESS. Check past and future issues of *2600* for complete details on how these systems work.

Operators

Another vital ingredient of the Network is the telephone operator. There are many different kinds. What follows is a discussion of some of the more common ones.

• **TSPS Operator.** The TSPS [Traffic Service Position System (as opposed to This Shitty Phone Service)] Operator is probably the bitch (or bastard for the phemale liberationists) that most of us are used to having to deal with.

Here are her responsibilities:

1) Obtaining billing information for Calling Card or 3rd number calls.

2) Identifying called customer on person-to-person calls.

3) Obtaining acceptance of charges on collect calls.

4) Identifying calling numbers. This only happens when the calling number is not automatically recorded by CAMA (Centralized Automatic Message Accounting) and forwarded from the local office. This could be caused by equipment failures (ANIF—Automatic Number Identification Failure) or if the office is not equipped for CAMA (ONI—Operator Number Identification).

(I once had an equipment failure happen to me and the TSPS operator came on and said, "What number are you calling *from*?" Out of curiosity, I gave her the number to my CO, she thanked me, and then I was connected to a conversation that appeared to be between a frameman and his wife. Then it started ringing the party I originally wanted to call and everyone phreaked out (excuse the pun). I immediately dropped this dual line conference!)

You shouldn't mess with the TSPS operator since she *knows* where you are calling from. Your number will show up on a 10-digit LED read-out (ANI board). She also knows whether or not you are at a fortress fone and she can trace calls quite readily. Out of all of the operators, she is one of the *most dangerous!*

• **INWARD Operator.** This operator assists your local TSPS ("0") operator in connecting calls. She will never question a call as long as the call is within *her service area*. She can only be reached via other operators or by a Blue Box. From a BB, you would dial KP+NPA+121+ST for the INWARD operator that will help you connect any calls within that NPA only.

• **DIRECTORY ASSISTANCE Operator.** This is the operator that you are connected to when you dial 411 or NPA-555-1212. She does not readily know where you are calling from. She does not have access to unlisted numbers, but she does know if an unlisted number exists for a certain listing.

There is also a directory assistance for deaf people who use Teletypewriters (TTY's). If your modem can transfer BAUDOT (45.5 baud—the Apple Cat can), then you can call him/her up and have an interesting conversation. The number is 800-855-1155. They use the standard Telex abbreviations such as GA for Go Ahead. They tend to be nicer and will talk longer than your regular operators. Also, they are more likely to be persuaded to give more information through the process of "social engineering".

Unfortunately, they don't have access to much. I once bullshitted with one of these operators and I found out that there are two such DA offices that handle TTY. One is in Philadelphia and the other is in California. They have approximately seven operators each. Most of the TTY operators seem to think their job is boring. They also feel they are underpaid. They actually call up a regular DA # to process your request—no fancy computers here! (Other operators have access to their own DA by dialing KP+NPA+131+ST (MF).

The TTY directory assistance, by the way, is still a free call, unlike normal DA. One might be able to avoid being charged for DA calls by using a computer and modem at 45.5 baud.

• **CN/A Operator.** CN/A operators do exactly the opposite of what directory assistance operators are for. You give them the number, they give you the name and address (Customer Name/Address). In my experiences, these operators know more than the DA operators do and they are more susceptible to "social engineering." It is possible to bullshit a CN/A operator for the NON-PUB DA # (i.e., you give them the name and they give you the unlisted number). This is due to the fact that they assume you are a fellow company employee. The divestiture, though, has resulted in the break-up of a few NON-PUB #'s and policy changes in CN/A.

• **INTERCEPT Operator.** The intercept operator is the one that you are connected to when there are not enough recordings available or the area is not set up to tell you that the number has been disconnected or changed. They usually say, "What number did you dial?" This is considered to be the lowest operator lifeform since they have no power whatsoever and usually know very little.

• **OTHER Operators.** And then there are the: Mobile, Ship-to-Shore, Conference, Marine, Verify, "Leave Word and Call Back," Route and Rate (KP+800+141+1212+ST—new number as a result of the break-up), and other special operators who have one purpose or another in the Network.

Problems with an Operator? Ask to speak to their supervisor...or better yet, the Group Chief (who is the highest ranking official in any office), the equivalent of the Madame in a whorehouse (if you will excuse the analogy).

Some CO's, by the way, have bugs in them that allow you to use a 1 or a 0 as the 4th digit when dialing. (This tends to happen mostly in crossbars and it doesn't work consistently.) This enables a caller to call special operators and other internal telco numbers without having to use a blue box. For example, 415-121-1111 would get you a San Francisco-Oakland INWARD Operator.

(The above was taken from Basic Telecommunications Part IV, *written by BIOC Agent 003.)*

Exploring Caves in Travelnet

One fine summer day several years ago, a phone phreak discovered yet another interesting telephone number. What was it? A modem? A dialtone? A very special operator? No to all of the above—*this* was something truly amazing and unique. This was TRAVELNET.

Of course, he didn't know at the time what he had dialed into. But this is what he heard. Two rings, a tone that lasted for about half a second (it had about the same pitch of a Sprint tone), and then a voice! Not just a recording, not just a human asking what it was you wanted, but a *recording* asking you what it was you wanted! Sort of like hearing an answering machine for the first time. But this was no answering machine.

"Authorization number, please," a sensual, husky female voice asked. And since he was a rather clever guy, he hit his touch tone® keypad. Every time he entered a tone, he heard a short "booop," like an acknowledgement of some sort. After four of these "booops" the automated lady came back and said "eighteightsevenzero." But, alas, those were not the keys he hit. In semi-desperation, he hit another key. The female voice came back and said, "Please repeat, yes or no?" But what was the question? He quickly realized that she must have been somehow trying to confirm the entry of his numbers. But how do you convey the word "no" on a touch tone® keypad?

He went through the whole process again and wound up getting dumped into a recording that said (in an authoritative female voice), "The Travelnet number you dialed is incorrect; please check the number and dial again."

He called back. Again he tried entering numbers and tried to figure out why they wouldn't correspond. All of a sudden, his baby sister (who had been growing increasingly bored with a rattle in the next room), decided to let out the sort of scream that baby sisters are known for. What's important about this is that after the scream was over, our friend heard quite distinctly over the telephone lines: "booop."

"Wow," he said. "Booop," it repeated. It recognized speech! He called it back and started entering numbers with his voice. It worked! After four numbers were entered, it would repeat them back to him and he had the option of saying either "yes" or "no". If he said "yes" or remained silent, he had the opportunity to enter four more numbers. If he said "no" the machine would make every effort to find out what the number was by asking him twice just what it was he meant to say. There were a few simple rules—he had to enunciate clearly and say the word "zero" instead of "oh".

But what would this lady let him do if he guessed the right eight numbers? And how could he possibly get such a long number anyway. Would he have to call up the lady and slowly and patiently pronounce little words over and over? Since he knew that there were over 100,000,000 possible combinations and that no more than a thousand probably worked, he understood that it would take some thinking to satisfy the mechanical voice. He needed to find some good old-fashioned human incompetence. If the machine had trouble hearing him, or if he remained silent, it would eventually say, "Sorry, we're having difficulties." Then it would connect him to a human. He stuck on the line and when the operator answered, he asked her what number he had dialed. "This is General Motors Travelnet, sir," she replied. "I'm terribly sorry," he said, "I was trying to get the speaking clock." "That's okay," the operator said, "Goodbye."

So it was General Motors! This would be easy. He waited a day and called back. He got connected to another operator, who asked him what he wanted. "This is J.C. Steppleworth from Fort Wayne GMAC," he snarled. "And I've been having trouble using this confounded phone system." "Well, why don't you call the instruction number, sir?" She gave him the number. He called this number and heard a full demonstration on how to use the system. It was used to make phone calls, which he sort of suspected. After you enter your eight-digit code, you enter a ten-digit phone number or, if dialing internally within General Motors, a seven-digit number. The recording even spoke a demo authorization code to get the point across. After hearing this, our friend wondered if he should try the demo code. "No," he decided, "They couldn't possibly be *that* stupid." He tried it anyway and guess what? The moment he confirmed the last number, the lovely voice asked a new question: "Destination code, please?" (In other words, the phone number you're trying to call.)

It was an extender—a long and short distance phone service. He proceeded to test it out, and he found that he could call virtually anywhere in the country for free. But who cares about free calls? He wanted to explore. And explore he did. He tried many things and learned many things. He found that he could avoid the lady's voice if he keypadded in the numbers before she could speak. This way the call would go through normally without any arguments on pronunciation. This allowed him to test many, many codes without much hassle. He found that by mixing up his working code a little, he was able to find many new ones. The simplicity was astounding. In a short time, he had found literally hundreds of codes. After this, he sat down one day and stared at his list of codes. All of a sudden, he realized something. Each group of four added up to either 9, 19, or 29—a sort of base-nine code. He wrote a short program and printed out all possible four-digit combinations that added up to these magic numbers. He was set for life.

He used the system to explore internal offices. If no area code was entered, every exchange put you in a different part of the country. One exchange, 999, simply dumped him into a feed from a Detroit radio station. One day, his Demon-dialer, which is basically a touch tone® generator with a memory, came across a re-order (a fast busy signal) that turned into a dialtone in twenty seconds. The connection wasn't great, but he found that he could make a direct call *anywhere*. He could dial overseas directly. He figured that he was at the switchboard of some office branch far away from where he originally called. He found out what the number was by calling a friend person-to-person collect, who then asked the operator for the number so that the "person" could call back when he returned. When he called up the number he was dialing from, they answered, "GMAC." So it was some distant office that he was making his calls out of, using a Travelnet code and an internal number to get there. It was so roundabout that he knew nobody would figure it out. In fact, several people that he called received calls from that office asking if they knew anybody who worked there that would call them at three in the morning. It was incredible! Even if a friend had *wanted* to frame him, it was doubtful that they would connect him with this distant city from which the call supposedly emanated. And the funny thing was that the company was probably placing a 24-hour armed guard on the building, thinking that someone was breaking in and making calls. Someone was, but in a way they could never figure out.

There's much more to the world of Travelnet, particularly on their internal network. And the same number works to this very day, which, by the way, is toll-free. But we've heard of cases where people have been trapped into paying for what they did and it's quite likely the system is heavily monitored.

A similar system called WIN was used by Westinghouse before they gave up in disgust after their lines were constantly tied up by phreakers and hackers. Honeywell makes the actual system and there are others in use around the country—one, we hear, for the state offices of Illinois, another for Ralston-Purina—the folks who blow up sewers in Louisville, KY.

As usual, nobody at Travelnet understood any of the questions we asked them and no one returned our calls. Maybe the lines were all tied up.

Fun With Fortress Fones

This article will focus primarily on the standard Western Electric single-slot coin telephone (aka fortress fone) which can be divided into 3 types:

- Dial-Tone First [DTF]
- Coin-First [CF] (i.e., it wants your money *before* you receive a dial tone)
- Dial Post-Pay Service [PP] (you pay after the party answers)

Depositing Coins (Slugs)

Once you have deposited your slug into a fortress, it is subjected to a gamut of tests.

The first obstacle for a slug is the magnetic trap. This will stop any light-weight magnetic slugs and coins. If it passes this, the slug is then classified as a nickel, dime, or quarter. Each slug is then checked for appropriate size and weight. If these tests are passed, it will then travel through a nickel, dime, or quarter magnet as appropriate. These magnets set up an eddy current effect which causes coins of the appropriate characteristics to slow down so they will follow the correct trajectory. If all goes well, the coin will follow the correct path (such as bouncing off of the nickel anvil) where it will hopefully fall into the narrow accepted coin channel.

The rather elaborate tests that are performed as the coin travels down the coin chute will stop most slugs and other undesirable coins, such as pennies, which must then be retrieved using the coin release lever.

If the slug miraculously survives the gamut, it will then strike the appropriate totalizer arm causing a ratchet wheel to rotate once for every 5 cent increment (e.g., a quarter will cause it to rotate 5 times).

The totalizer then causes the coin signal oscillator to readout a dual-frequency signal indicating the value deposited to ACTS (a computer) or the TSPS operator. These are the same tones used by phreaks in the infamous red boxes.

For a quarter, 5 beep tones are outpulsed at 12-17 pulses per second (PPS). A dime causes 2 beep tones at 5-8.5 PPS while a nickel causes one beep tone at 5-8.5 PPS. A beep consists of 2 tones: 2200 + 1700 Hz.

A relay in the fortress called the "B relay" (yes, there is also an "A relay") places a capacitor across the speech circuit during totalizer readout to prevent the "customer" from hearing the red box tones.

In older 3 slot phones, one bell (1050-1100 Hz.) for a nickel, two bells for a dime, and one gong (800 Hz.) for a quarter are used instead of the modern dual-frequency tones.

TSPS and ACTS

While fortresses are connected to the CO of the area, all transactions are handled via the Traffic Service Position System (TSPS). In areas that do not have ACTS, all calls that require operator assistance, such as calling card and collect, are automatically routed to a TSPS operator position.

In an effort to automate fortress service, a computer system known as Automated Coin Toll Service (ACTS) has been implemented in many areas. ACTS listens to the red box signals from the fones and takes appropriate action. It is ACTS which says, "Two dollars please. (pause) Please deposit two dollars for the next ten seconds..." and other variations. Also, if you talk for more than three minutes and then hang up, ACTS will call back and demand your money. ACTS is responsible for Automated Calling Card Service, too.

In addition, ACTS provides trouble diagnosis for craftspeople (repairmen specializing in fortresses). For example, there is a coin test which is great for tuning up red boxes. In many areas this test can be activated by dialing 09591230 at a fortress (thanks to Karl Marx for this information). Once activated it will request that you deposit various coins. It will then identify the coin and outpulse the appropriate red box signal. The coins are usually returned when you hang up.

To make sure that there is actually money in the fone, the CO initiates a "ground test" at various times to determine if a coin is actually in the fone. This is why you must deposit at least a nickel in order to use a red box!

Green Boxes

Paying the initial rate in order to use a red box (on certain fortresses) left a sour taste in many red boxer's mouths. Thus the *green* box was invented. The green box generates useful tones such as COIN COLLECT, COIN RETURN, and RINGBACK. These are the tones that ACTS or the TSPS operator would send to the CO when appropriate. Unfortunately, the green box cannot be used at a fortress station but it must be used by the *called* party.

Here are the tones:

COIN COLLECT	**700 + 1100 Hz.**
COIN RETURN	**1100 + 1700 Hz.**
RINGBACK	**700 + 1700 Hz.**

Before the called party sends any of these tones, an operator released signal should be sent to alert the MF detectors at the CO. This can be accomplished by sending 900 + 1500 Hz. or a single 2600 Hz. wink (90 ms) followed by a 60 ms gap and then the appropriate signal for at least 900 ms.

Also, do not forget that the initial rate is collected shortly before the 3 minute period is up.

Incidentally, once the above MF tones for collecting and returning coins reach the CO, they are converted into an appropriate DC pulse (-130 volts for return and +130 volts for collect). This pulse is then sent down the tip to the fortress. This causes the coin relay to either return or collect the coins.

The alleged "T-Network" takes advantage of this information. When a pulse for COIN COLLECT (+130 VDC) is sent down the line, it must be grounded somewhere. This is usually either the yellow or black wire. Thus, if the wires are exposed, these wires can be cut to prevent the pulse from being grounded. When the three minute initial period is almost up, make sure that the black and yellow wires are severed, then hang up, wait about 15 seconds in case of a second pulse, reconnect the wires, pick up the fone, hang up again, and if all goes well it should be *jackpot* time.

Physical Attack

A typical fortress weighs roughly 50 pounds with an empty coin box. Most of this is accounted for in the armor plating. Why all the security? Well, Bell attributes it to the follwing:

"Social changes during the 1960's made the multislot coin station a prime target for: vandalism, strong arm robbery, fraud, and theft of service. This brought about the introduction of the more rugged single slot coin station and a new environment for coin service."

As for picking the lock, I will quote Mr. Phelps: "We often fantasize about 'picking the lock' or 'getting a master key'. Well, you can forget about it. I don't like to discourage people, but it will save you from wasting a lot of your time—time which can be put to better use (heh, heh)."

As for physical attack, the coin plate is secured on all four sides by hardened steel bolts which pass through two slots each. These bolts are in turn interlocked by the main lock.

One phreak I know did manage to take one of the "mothers" home (it was attached to a piece of plywood at a construction site; otherwise, the permanent ones are a bitch to detach from the wall!). It took him almost ten hours to open the coin box using a power drill, sledge hammers, and crow bars. It turned out to be empty...perhaps next time, he'll deposit a coin first to hear if it slushes down nicely or hits the empty bottom with a clunk.

Taking the fone offers a higher margin of success, although this may be difficult, often requiring brute force. There have been several cases of back axles being lost trying to take down a fone! A quick and dirty way to open the coin box is by using a shotgun. In Detroit, after ecologists cleaned out a municipal pond, they found 168 coin phones rifled.

In colder areas, such as Canada, some shrewd people tape up the fones using duct tape, pour in water, and come back the next day when the water will have frozen, thus expanding and cracking the fone open.

In one case, "unauthorized coin collectors" were caught when they brought $6,000 in change to a bank and the bank became suspicious....

At any rate, the main lock is an eight level tumbler located on the right side of the coin box. This lock has 390,625 possible positions (5^8, since there are 8 tumblers each with 5 possible positions), thus it is highly pick resistant! The lock is held in place by 4 screws. If there is sufficient clearance to the right of the fone, it is conceivable to punch out the screws with a drill.

Miscellaneous

In a few areas (rural and Canada), post-pay service exists. With this type of service, the mouthpiece is cut off until the caller deposits money when the called party answers. This also allows for free calls to weather and other dial-it services, where it's not necessary for you to talk. In July, *2600* announced the "clear" box which consists of a telephone coil and a small amp. It is based on the principal that the receiver is also a weak transmitter and that by amplifying your signal you can talk via the transmitter thus avoiding costly telephone charges!

Most fortresses are found in the 9xxx area. Under former Bell areas, they usually start at 98xx (right below the 99xx official series) and move downward.

Since it's the line and not the fone that determines whether or not a deposit must be made, DTF and Charge-A-Call fones have been known to make great extensions!

Finally, fortress fones allow for a new hobby—instruction plate collecting. All that is required is a flat-head screwdriver and a pair of needle-nose pliers. After all, ten cent plates are definitely becoming a "rarity"!

Fortress Security

While a lonely fortress may seem the perfect target, beware! The Gestapo have been known to stake out fortresses for as long as 6 years according to the *Grass Roots Quarterly*. To avoid any problems, do not use the same fones repeatedly for boxing, calling cards, and other experiments. The telco knows how much money should be in the coin box and when it's not there they tend to get perturbed (read: pissed off).

(The above was excerpted from BIOC Agent 003's course in Basic Telecommunications, Part VI. Neither BIOC nor this magazine advocates doing anything illegal with regard to phones or any other type of machine. Further information available on dataline 9143591517.)

A Time For Reflection

1984 will not go down in history as the year of the phone phreak or computer hacker. Instead it will most likely be labeled something dumb like the year of the communications revolution or the PC bonanza. That's not surprising at all; those are precisely the things that *appeared* to have occurred this year. But we know better.

The true communications revolution has been going on for quite some time. Many years ago, the first telephone enthusiasts started using their phones to do a little more than just call people they knew. They began to experiment. They sent strange tones down the line, activated distant machines, and traded information among themselves. Not only that, but they took it upon themselves to learn all about the intrastructure of the biggest company on earth, Ma Bell. Now almost everyone knows something about the way the giant phone company used to work and the way the near-giants work today. All you hear now is talk of long distance services and how great each one is. All you see advertised everywhere are telephones, as if they'd just been invented. Which, in a way, they have been. For the average person. Others, though, have been participating in this "revolution" for quite some time.

A similar story holds true for computers. The field is exploding now on Madison Avenue. But all of this talk of floppies, K, megabytes, and control-c's is old news to hackers (both the programming and the cracking kind). As a rule, they've been into this kind of thing for years.

So what are we saying here? Two things, really. Looking at the past, it's pretty clear that those "mischief-makers" weren't only interested in causing chaos and perpetrating fraud, but also in being among the first to try their hand at the new technology, without being hovered over and told what not to do. Our other point lies with the future. Those phone phreaks and computer hackers of today may still be in a position to shine the light in front of the masses. We had at least one example of that in 1984, when hackers uncovered the wealth of information that is stored in the TRW computers—personal information about almost everyone that can be looked at by almost anyone. A glance at this year's pages of *2600* reveals a disturbing number of Orwellian touches in the works—cameras surveying streets for possible crimes, vastly expanded FBI files on innocent people, neat categorization of human beings.... Technological enthusiasts aren't the only kind of people that can find these nasty things in their beginning stages. But these days, they can sure be one of the most important. Happy new year.

MCI Mail

Easy Link℠

We here at *2600*, and apparently many of you, have been having problems with two of the biggies in the E-Mail business—namely MCI Mail and Western Union Easylink.

Let's start with the Easylink tale. Many many months ago, we saw a great big ad someplace inviting us to sign up for this wonderful electronic mail service. There were no minimum charges of any kind and there was no fee to sign up, so we gave them a call. Only after they got us started did they bother to mention that there was a $25 monthly minimum after the first 3 months. Because of this, and also because of the fact that their prices aren't that great, we stopped using their system. Since the service we signed up for was advertised as "free", we were under no obligation to cancel the account. Sure enough, after the third month had passed, we received a ten-page bill for $25. That's right, a ten-page bill. They believe in itemizing your use of the system in as many different ways as they can think of. The fact that we didn't use the system at all didn't stop them from itemizing our non-use.

Every month, like clockwork, that Easylink bill comes, with $25 more added each time. It's well into the triple digits now. Occasionally we get a mailgram asking why we haven't used the system in such a long time, but we have yet to get a letter asking why the hell we haven't paid our bill. In addition to these charges for answering a misleading advertisement, we get plenty of solicitations to use their many other expensive services and even to get an additional account.

Finally, the Easylink people, or machines, have been kind enough to send us roughly 20 pounds of Western Union directories and user guides. In fact, we often receive duplicate directories together with the useless bill. What a big pile all this stuff makes!

As an addendum, you may note that Easylink still offers free accounts with no minimum usage in most of their advertising.

And in the other corner...

But our real trouble is or was with MCI Mail, those other bozos. Last month, we told you about how our account was inactivated. In fact, we later found out through our own detective work that our account was "accidentally" deleted instead of being reactivated. Whoops! We were also told that the slobs at McMail were sorry. They also added that all of our inbound mail for the last month and a half was destroyed (they don't keep backups, they claim, seemingly proud of the fact). When we asked about recompense for us or for our correspondents for lost business and for those who were charged for mail that wasn't ever received, they insisted that they did not charge for mail that wasn't read. We doubt that this is true, but we cannot get ahold of their billing records or records of the mail that we did not receive, so we cannot prove otherwise. But we can advise you not to pay for any mail you may have sent to us, because odds are we never received it. Remember, they assured us that they couldn't give us the deleted mail or any other information, so *you* are the only one who knows if you sent us anything. By the way, if you request a refund, you'll probably have to make a voice call to a human since their customer service mail account (MCIHELP) has also been deleted for your inconvenience.

We raised quite a stink about this escapade, and even sent a letter to the president of MCI! It took him three business days to read *his* electronic mail and all we got out of him was a copy of a message he sent to the president of MCI Mail, who had apparently "explained" the situation to him. It read: "Thanks for the info. There must be hundreds of them. My condolences." This pretty much confirms our suspicions. MCI Mail has a blacklist which they've developed through reading their subscribers' private mail. If they see anything they don't like or if you get mail from someone they don't like—bang! You're on the list. Of course, there's no way to prove this. Electronic mail is very easy to reseal. What's more, they're not breaking any laws because they own the system.

We managed to get a new account that's now working, but we don't plan on keeping it and we don't advise anyone else to subscribe at this point. Starting next year, MCI Mail will be charging a yearly fee of $18 as well as charging for access to their 800 toll-free dialup. Perhaps E-COM will soon have company.

Trick of the month: MCI Mail allows you to send telex messages all over the world. But if you send to a nonexistent telex in some remote country, it will eventually come back and say that the telex couldn't be found. When that happens, there's no charge! And you just know they've gone to an awful lot of trouble!

The Scariest Number in the World

Recently, a telephone fanatic in the northwest made an interesting discovery. He was exploring the 804 area code (Virginia) and found out that the 840 exchange did something strange. In the vast majority of cases, in fact in *all* of the cases except one, he would get a recording as if the exchange didn't exist. However, if he dialed 804-840 and four rather predictable numbers, he got a ring!

After one or two rings, somebody picked up. Being experienced at this kind of thing, he could tell that the call didn't "supe", that is, no charges were being incurred for calling this number. (Calls that get you to an error message, or a special operator, generally don't supervise.) A female voice, with a hint of a Southern accent said, "Operator, can I help you?"

"Yes," he said. "What number have I reached?"

"What number did you dial, sir?"

He made up a number that was similar.

"I'm sorry, that's not the number you reached." Click.

He was fascinated. What in the world *was* this? He knew he was going to call back, but before he did, he tried some more experiments. He tried the 840 exchange in several other area codes. In some, it came up as a valid exchange. In others, exactly the same thing happened—the same last four digits, the same Southern belle. Oddly enough, he later noticed, the areas it worked in seemed to travel in a beeline from Washington DC to Pittsburgh, PA.

He called back from a payphone. "Operator, can I help you?"

"Yes, this is the phone company. I'm testing this line and we don't seem to have an identification on your circuit. What office is this, please?"

"What number are you trying to reach?"

"I'm not trying to reach *any* number. I'm trying to identify this circuit."

"I'm sorry, I can't help you."

"Ma'am, if I don't get an ID on this line, I'll have to disconnect it. We show no record of it here."

"Hold on a moment, sir."

After about a minute, she came back. "Sir, I can have someone speak to you. Would you give me your number, please?"

He had anticipated this and he had the payphone number ready. After he gave it, she said, "Mr. XXX will get right back to you."

"Thanks." He hung up the phone. It rang. *Instantly!* "Oh my God," he thought, "They weren't asking for my number—they were *confirming* it!"

"Hello," he said, trying to sound authoritative.

"This is Mr. XXX. Did you just make an inquiry to my office concerning a phone number?"

"Yes. I need an identi—"

"What you need is advice. Don't ever call that number again. Don't even think about calling that number again. Forget you ever knew it."

At this point our friend got so nervous he just hung up. He expected to hear the phone ring again but it didn't.

Over the next few days he racked his brains trying to figure out what the number was. He knew it was something big—that was pretty certain at this point. It was so big that the number was programmed into every central office in the country. He knew this because if he tried to dial any other number in that exchange, he'd get a local error message from his CO, as if the exchange didn't exist.

It finally came to him. He had an uncle who worked in a federal agency. He had a feeling that this was government related and if it was, his uncle could probably find out what it was. He asked the next day and his uncle promised to look into the matter.

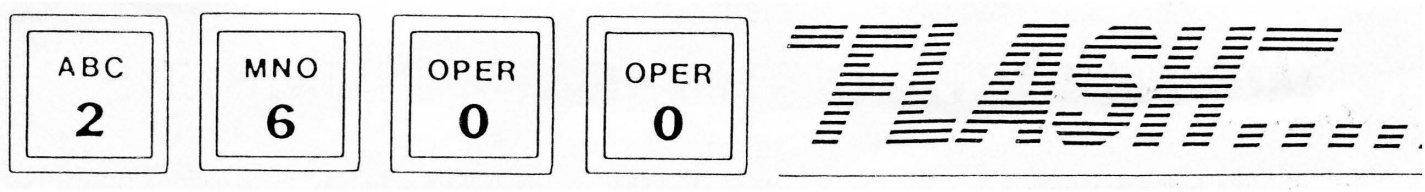
The next time he saw his uncle, he noticed a big change in his manner. He was trembling. "Where did you get that number?!" he shouted. "Do you know I almost got fired for asking about it?!? They kept wanting to know where I got it!"

Our friend couldn't contain his excitement. "What is it?" he pleaded. "What's the number?!"

"It's the President's bomb shelter!"

He never called the number after that. He knew that he could probably cause quite a bit of excitement by calling the number and saying something like, "The weather's not good in Washington. We're coming over for a visit." But our friend was smart. He knew that there were some things that were better off unsaid and undone.

(If you have a phone or computer story, call or write us!)



The very first issue of *2600* had a news section that was called "*2600* Flash." The collection of stories, and the commentary that often went along with them, quickly became one of the more popular parts of the publication and it appeared in every issue of 1984. Stories were gathered from a variety of sources and, in some cases, investigated by *2600* staffers under the credit of "*2600* News Service," "Word of Mouth," or even "A Friendly Information Operator." On one occasion in June, a story that hit particularly close to home ("*2600* Writer Indicted") was made bold and surrounded by a box.

January 1984

GTE raids still have many unanswered questions—computer owners concerned

Combined News Sources

On Wednesday, October 12, at 6:00 AM, the FBI started to raid the homes of over fifteen individuals for allegedly breaking into Telemail, GTE Telenet's massive electronic mail service. While much of the publicity has now died down, questions remain concerning the legality and the overall implications of such computer seizures.

At a December 16 meeting of the Long Island Computer Association, this topic was addressed. Some members could not understand the rationale for taking away the computers in the first place. "It sounds like scare tactics to me... to keep these kids off of computers," one commented. "To hold the equipment seems like something that should be unlawful and it's something that the public should look at. If it's not justified, we should say that we won't put up with it anymore and to return the equipment." He did not elaborate on precisely what kind of action a computer group such as LICA could take.

Legally, the computers can be kept for as long as they are needed in the investigation. Ultimately, a judge will decide how long that can be.

"The allegation," said an attorney familiar with the case, "is that the services of the Telemail bulletin boards were used and the theory that the government is proceeding under is that it was a violation of Section 1343, wire fraud (a scheme with intention to defraud someone else using either television, telephone, or some other communications means). They're saying that if there was use of the bulletin board service, then that was a 'theft of service' and there was intention to defraud GTE."

One member took GTE's side. "These are all nice games these people are playing, but they are a theft of service. Somebody is in the business of providing that service and they're deliberately interfering with their providing that service. They're trying to get something for nothing."

Another disagreed. "You may be on their computer, but it's not costing them anything, if you're not taking up time. Unless the whole system is fully used and you were the last user on, are you really using any of their time? Really and truly?"

Many hackers felt they were unjustly accused. One even said he'd never used the Telemail system. Others said they had looked around once or twice but had never hurt anything. Others, though, admitted to deleting mail and playing tricks, like sending obscene messages back and forth between two innocent executives.

Whether or not the Telemail system was used fraudulently did not seem to be the overriding issue at the LICA meeting. What had members there worried was the way in which the investigation was being carried out. When dealing with computers as evidence, different rules apply, rules that for the most part have not been written yet. "Data can be manufactured just as easily as it can be erased from a personal computer," one member commented. "And the longer that they have the computer in their custody, the less likely that the information that they claim is on it was actually there. Because, as we know, you could enter any date, any time into the computer and have it date- and time-stamp the files."

Meanwhile, a GTE Telenet spokesperson said that the corporation still intends to prosecute and denied that the whole thing was being put on for the deterrent effect that it might have on other people. The spokesperson also said that abuse on the system was discovered in the past, but they didn't prosecute at that time. This time, though, they're serious.

AT&T Credit Cards Make Debut

2600 News Service

There's now another way to place telephone calls without dimes. This month, the "true" AT&T credit card phones are making their debut in various airports around the country. This new phone actually takes an AT&T credit card (not those wimpy "calling cards" or "PIN cards." We're talking about a *real* hunk of plastic, with a magnetic strip and everything.) — and there's even a little video screen that gives you directions.

Unless some sort of a bug can be found within the system itself, phone phreaks won't accomplish very much here, unless they can actually get their hands on other people's cards. This, in itself, wouldn't be too difficult, since large numbers of the cards would be sent out on the same day in a particular area. Stealing out of personal mailboxes, though, is an act most phone phreaks would never stoop to. And the folks at AT&T are well aware of this.

Wireless phones spell trouble

2600 News Service

With cordless phones popping up all over the place, problems were bound to arise. It's not at all uncommon to hear another cordless conversation on your phone or to hear the electronic pulse-beeping when you're not even dialing. Then there are cordless phone phreaks to deal with, who drive into heavily populated zones holding one of the common cordless models. It's called "cruising for dialtones." And some phones are nice enough to broadcast your conversation on an AM frequency. This feature isn't very good for private conversations. It helped shape a recent drug bust in the state of New York.

Recently, a lady in the Midwest called up her local electric company to tell them that she was going to be away for two months. A member of the 2600 Club heard this on his radio and, being in a good mood, called her and told her that important, personal business should *never* be discussed on cordless phones. After thanking him, she exclaimed, "That thing's going right back to the Phonecenter Store!"

1984 arrives in Hong Kong

The Los Angeles Times

In an effort to "discourage people from driving their cars in heavily congested areas" all 350,000 of Hong Kong's motor vehicles will be fitted with tracking devices that will let government computers know exactly where each car has traveled so that the owner can be billed for road use. This system could be in full implementation by 1987, if the government has its way. Such a system would also allow the police to quickly pinpoint the whereabouts of any vehicle. Tampering with the $45 tracking devices will be illegal and any attempt to do so will trigger street cameras to photograph the license plate of the car.

February 1984

Times Changing For Directory Assistance

Combined News Sources

Directory Assistance promises to have a very different future, both in the U.S. and in France. Here in the States, customers are being threatened with a 75¢ charge for long distance information requests. In a few parts of the country, Indiana (812) for instance, a request for a phone number produces startling results: a human will answer and ask for the city and name, and after finding it will hit a button, whereupon a machine takes over and spits out the number with a digitized voice. You are then given the option to hold on to be reconnected to another D.A. operator.

This kind of system makes multiple requests quite inconvenient—forcing one to either wait to be reconnected to a human, or dial over and over again. This latest step towards *total* mechanization also strikes fear into the hearts of the D.A. operators, many of whom do not wish to lose their fun jobs.

France, meanwhile, has a nationalized phone system run by the Ministry of Posts and Telecommunications, an agency which has been experimentally offering computerized telephone information (Teletel) to 70,000 users. The Ministry provides, for free, a small terminal called a Minitel which has a keyboard that folds up over the screen.

To find a number, a user enters the name, address, region of France, and profession of the person they're looking for. If just the name and city are entered, all of the people with that name in that city will be displayed. The system does not yet list all of France, but should by June. The Ministry expects to have 3 million terminals in use within two years. In addition to Teletel, 15 other services will be provided, including news, stock quotations, shopping catalogs, banking systems, as well as railroad, airline, and movie schedules.

Perhaps this will give AT&T some ideas. Imagine being able to call a distance city and get phone numbers for everybody named Smith! Electronic phone book hacking could be a considerable amount of fun.

No Hacking While Flying, Please

Combined News Sources

Eastern Airlines now specifically prohibits the use of portable computers on all flights, because of adverse effects the airline claims may occur. The new baggage policy excludes calculators from this ban.

The feeling at Eastern is that portable computers can interfere with radar and "distort equipment," causing all kinds of strange things to happen. When a company spokesperson for the Miami based carrier was asked if any specific incident triggered the new policy, she responded that an incident "probably happened" but that nothing more could be said.

A possible boycott of the airline has been proposed by Wayne Green, publisher of the magazine *Microcomputers*.

Trick of the Month

2600 News Service

Many supermarkets in states having passed a "bottle bill" of sorts are installing can-return machines. You put an empty aluminum soda can in the machine, UPC code up, and the machine crunches it and gives you money. Well, some hackers have discovered that these machines work for *all* beverage cans, deposit or not. In some states, for example, non-carbonated beverages (iced tea) don't carry a deposit even though the cans are exactly the same as the ones containing carbonated drinks. A human will not take those cans back, but the machines will, gladly.

By the way, we haven't heard from anyone who's tried putting a *full* soda can in one of these machines. It would be interesting to find out if the machine tries to crush it. More interesting to see if it succeeds.

Death Star Cards Spell Woe

2600 News Service

Many of the long-awaited AT&T credit cards are now being distributed. You will be impressed when you get yours—complete with a picture of the AT&T death star floating over planet Earth, while the new AT&T red, blue, and black stripe looks on.

But with these cards come a few problems. For one thing, many customers of New York Telephone received their PIN cards only days before they got their AT&T cards. What is a PIN card? Well, PIN stands for Personal Identification Number, but other than that, it's really the exact same thing as an AT&T card, except that it doesn't have a magnetic stripe. It also only has four numbers on it—the last part of your 14-digit code (your phone number comprises the first part). New York Telephone proudly claims that this secures your code, since if you lose your card, whoever finds it won't know your phone number nor be able to find out because your name isn't even on it. So along comes AT&T sending out *their* cards to everyone who got a PIN card. AT&T cards have your name *and* your 14-digit code prominently displayed (yes, the last four digits are the same as New York Telephone's). Result: the PIN cards are completely useless, both because they're redundant and because their purpose has been defeated.

AT&T has made a serious mistake with these cards. First of all, since so many of them are in the mail at the same time, many will be stolen, perhaps within the post office itself. Second, there are *no* security precautions whatsoever at those new credit card phones. You simply plug in the card and dial away. No identity codes to enter, like the bank cards require. With 5,000 of these phones (which also accept American Express cards) scheduled to be installed this year, credit card fraud for AT&T will almost certainly rise, not so much due to phone phreaks, but rather, simple common thieves.

An official at AT&T said that they were not overly concerned. "We're counting on people's honesty," they said. We'll see what they say next year.

ADS Investigation Moved?

Word of Mouth

It's been rumoured that the FBI investigation of IBM Audio Distribution System hackers has now been headquartered in another city (i.e. *not* Detroit). Last month, *2600* published a rather extensive report on the investigation, including the name of the city and the informant who started this whole mess, John Maxfield of JFM Industries in Detroit.

Several threats have allegedly been made by Maxfield to a group of hackers who helped expose him. This is reportedly being done against the wishes of the FBI. *2600* is currently investigating the authenticity of these threats and, if they check out, you can count on seeing a transcript next month.

March 1984

718 is coming!

The New York Times

The New York State Public Service Commission has voted to begin dividing New York City into two area codes on September 1 to "prevent an impending exhaustion of telephone numbers." At that time, the old 212 area code will begin to reach only Manhattan and the Bronx, whereas a brand new area code, 718, will start to work for Brooklyn, Queens, and Staten Island. The whole system becomes mandatory on January 1, 1985.

Charles Herndon, a New York Telephone spokesman, said that the 718 code was assigned to the city years ago by the North American Dialing Plan, a group that administers area codes in the U.S., Mexico, and Canada.

"Of the numbers available at the time, 718 was the best," he said. "There weren't that many available."

The P.S.C. rejected recommendations by a consultant (Economics and Technology, Inc.) hired by the City Board of Estimates. Those recommendations called for the implementation of the 718 area code, however, instead of using it for people, the consultant suggested using it exclusively for computers, paging systems, and other devices, since they were the main reason for the new area code in the first place.

[*2600* would like to go on record as enthusiastically supporting the idea of an entire area code of machines.]

Supercomputer dialups

Physics Today

Astronomy and astrophysics are gathering so much data by telescope these days, that it cannot be handled by conventional computers, according to Dr. Vincent Icke of the University of Minnesota.

To remedy the problem, Dr. Icke called for the creation of a central supercomputer facility that would be at the disposal of all astronomers and astrophysicists nationwide via telephone lines.

Wiretap City

The New York Times

After an investigation, the New Haven (Connecticut) Board of Police Commissioners, a civilian body that oversees the Police Department, revealed in 1978 that the department had routinely tapped the phones of residents from 1964 to 1971, apparently to monitor radical political activity. This, the board said, was illegal.

In December 1982, after it had been disclosed that the phones of some 3000 residents had been tapped, the Federal District Court in Bridgeport made the case a class action, inviting anyone who felt wronged to become a plaintiff.

So far, 1230 people have become plaintiffs. They include several judges, lawyers, and other prominent political figures and, of course, a great many members of the Yale faculty.

Students Cause Havoc in Computer

Combined News Sources

A group of students at Gompers Secondary School in San Diego tapped into the school's computer system last month, causing all kinds of problems.

"It was funny at first when the kids changed the passwords so the teachers couldn't get into their programs in the system," said Alex Rascon, a school official. "But then they started deleting grades, altering the other kids' homework, and tampering with the teachers' files.

"These kids are whizzes—they're very bright," he went on. "Fortunately we caught it before too much damage was done. At this point it can be easily corrected."

Albert Cook, the assistant San Diego superintendent, took the sorehead approach. "We still haven't decided whether charges will be filed with the San Diego Police Department," he said.

The Person Numbers

The Associated Press

Sweden's Person Number is a 10-digit figure that tells who you are, where and when you were born, and your sex. Every computer file in the country is based on the Person Number, whether it's at a bank, a hospital, an employer, the social welfare office, or the tax authorities.

Person Numbers went into effect on January 1, 1947 and were computerized 20 years later. Recently, a government study suggested the creation of a super-databank (based on the Person Number) that the Central Bureau of Statistics could use freely. By calling up a Person Number on a terminal, the bureau would be able to find out details on everything from a person's illnesses and criminal record to his income and debts.

Critics of the plan see this as an erosion of civil liberties. One said, "The files will collect more information on a person than he can remember himself."

Furthermore...

2600 News Service

- All computers seized by the FBI last October during the Telemail raids have either been returned already or are in the process of being sent back. New developments in the case are expected shortly.
- Telenet now hangs up after 3 connection attempts, whether they're successful or not. This means that last month's article (*Hacking on Telenet*) is already slightly outdated, but only until somebody figures out a way around this latest hurdle.
- Some more signs of the divestiture—this time it's the 950 exchange. This is a universal exchange that is (or will soon be) working *everywhere*. 950-1022 and 950-1088 give alternate long distance dialtones. (The latter belongs to Skyline.) The connection is crystal clear and toll-free. Eventually, the 950 will be dropped and you will dial 10XX to make long distance calls, where XX is the carrier of your choice. You can't access 950's in other area codes.
- Eastern Airlines has changed its mind about allowing portable computers on flights, leaving only American Airlines maintaining the ban.
- 202 and 214 now have automated directory assistance too. Have you checked your area code today?

April 1984

Bell Credit Card Abuse Soars

2600 News Service

Huge phone bills are being sent to innocent people all over the country. So huge, in fact, that they can't be sent in envelopes—they come in boxes. In the past month and a half, this scene has begun to proliferate.

As predicted on these pages in February, the AT&T death star cards are creating all kinds of problems. All that anyone has to do is glance at one of them to obtain a valid AT&T code. And that's exactly what people are doing. Some of these folks are, in fact, so organized that the codes are used for practically 24 hours a day, with new calls starting as often as 3 times a minute from all different parts of the country. It's rapidly becoming one of the easiest ways to make free phone calls, and best of all, it's through an old friend: Ma Bell!

While AT&T has put itself in a rather vulnerable position, they are not completely without defense. Any time that a credit card call is placed, the number that the call is being placed *from* is recorded and sent to the customer. Most phreaks know enough not to do this kind of thing from their home or local payphone.

Meanwhile, there is a major crackdown underway in Las Vegas concerning unauthorized use of MCI, Sprint, and ITT (AT&T is rumoured to also be involved here). It seems that hundreds of people in that gambling town were passing codes around. The FBI claims that the persons involved are *not* phone phreaks, but that phreakers and hackers may have been hired to do the actual code-finding.

Electronics Create Portable Prisons

The New York Times

Cesario Romero, a 23-year-old New Mexico truck driver, recently served a 30 day sentence for disobeying a police officer. He never had to leave his home.

Romero was confined at home by a plastic box the size of a cigarette package that was strapped to his ankle. This device emits radio signals which would have informed the authorities if Romero strayed more than 150 feet from his telephone. The anklet emits a radio signal every 30 to 90 seconds which is picked up by a small receiver connected to the telephone outlet in the wearer's home. The receiver relays the signal to a computer that is monitored by the authorities. The printouts indicate each time the wearer exceeds the 150-foot limit and each time he tries to remove the anklet or unplug the receiver.

District Attorney Steven Schiff of the Second Judicial District said, "For someone like a first-time shoplifter, it could be used as a mild punishment, requiring the person to stay home nights and weekends for a specified time."

The U.S. Justice Department has expressed an interest in this monitoring system.

414's Plead Guilty

The Associated Press

Two young men, both members of the 414 computer enthusiasts group, pleaded guilty to two misdemeanor charges on March 16.

Gerald Wondra of West Allis, WI and Timothy D. Winslow of Milwaukee, both 21, broke into large computers in the U.S. and Canada last June, simply to prove that they could do it. The two agreed to plead guilty to two counts each of making harassing telephone calls, which is the most they can be charged with, since the government has no law against computer crimes. Each count carries a maximum penalty of six months in jail and a $500 fine.

The computers involved were located at: Security Pacific National Bank in Los Angeles, Memorial Sloan-Kettering Cancer Center in New York, Canada Cement LaFarge Inc. in Vancouver, BC, and Citadel Industries, a New Jersey corporation.

Teller Machine Crime Coming

The Los Angeles Times

The Justice Department says that automated teller machines and other means of electronic financial transactions are "potentially fertile for criminal abuse."

Techniques for robbing the systems already have cropped up and are expected to increase. They range from the dynamiting of an automatic teller device to the withdrawal of funds by a cardholder who then claims no knowledge of the transaction. Because of an absence of sophisticated verification procedures in today's automated teller systems, such as fingerprints or voiceprints, the door is wide open to unscrupulous cardholders committing fraud from their very own accounts. (Some machines, though, take a picture of the person as soon as he takes the cash.)

Even though bank officials may be skeptical of a cardholder's disclaiming any knowledge of a withdrawal that had been made from his or her account, federal law makes it difficult for the officials to reject such a claim. If a bogus loss is reported within two business days, the law makes the cardholder responsible for only the first $50.

Free Information in Trouble

The Associated Press

According to company spokesman Pic Wagner, AT&T is probably going to propose a 50-cent fee for long distance information calls instead of the 75-cent fee it proposed last fall. Consumers currently don't pay anything for long distance or overseas directory assistance.

A Word on Wiretapping

Long Island Newsday

A recent article by Lenny Siegel, director of the Pacific Studies Center in Mountain View, CA, dealt with the subject of wiretapping.

In this article, Siegel says, "Present law outlaws 'aural' (voice) wiretapping, the monitoring of telephone conversations, without judicial approval, but 'nonaural' surveillance is legal. Law enforcement and intelligence agencies can and do record telephone dialing information—who's calling whom—and digital data transmissions—messages between computers and other electronic devices. In fact, the General Accounting Office, an investigative arm of Congress, warns that existing legislation may permit listening in on the growing percentage of voice transmissions that have been converted to digital pulses within the telephone network."

May 1984

A 414 is Sentenced—Others Indicted

Combined News Sources

Twenty-one year old Gerald Wondra of West Allis, Wisconsin, was placed on two years' probation after pleading guilty to two misdemeanor counts involving computer cracking. Wondra, a member of the 414's, was accused of gaining access last summer to computers at the Security Pacific National Bank in Los Angeles and the Memorial Sloan-Kettering Cancer Center in New York, by using Telenet.

U.S. District Judge Terence T. Evans, in handing down the sentence, said, "It's important to send a message to Mr. Wondra and all others that this is a serious offense... with serious consequences." In other words, someone might go to *jail* the next time.

That next time may be coming soon. Four indictments were handed down on May 7th against people who allegedly were hacking the Telemail system last year. The four are located in California, Iowa, Illinois, and New York. Each is being charged with up to ten counts of wire fraud. Reliable sources say this is the first time that the wire fraud charge has been used to prosecute computer hackers.

Long Distance Option Timetable

USA Today

On July 15, Charleston, West Virginia will become the first city in the United States to offer equal access to alternate long distance companies. Equal access is part of the court-ordered breakup of the Bell system—most parts of the country should have it within three years.

What the people in Charleston will do is decide on a long distance company they want to use. Every long distance call they make will then be billed through that company. If the company they picked isn't AT&T, they can still use AT&T by notifying an operator first.

The main advantage here for the other companies is that they will no longer be getting inferior lines and that customers with rotary dial phones will be able to use their system without installing extra equipment.

Some cities and when they'll be doing this: Minneapolis, August 19; Mobile, Alabama, August 27; Indianapolis, August 30; Houston and Chicago, August 31; Milwaukee, New York City, Philadelphia, Baltimore, Washington, and Detroit, September 1.

Intelpost an Astronomical Failure

Jack Anderson

Intelpost was announced in 1978 by the U.S. Postal Service as an experiment to test delivery of electronic messages overseas by satellite. It was supposed to give businesses and individuals a quick, cheap way to send letters abroad from five major cities: New York, Washington, Chicago, Houston, and San Francisco.

The service is quick enough. But it is far from cheap. At a cost to the sender of $5 a page, customer reaction was predictable—to everyone but the Postal Service, that is.

A report issued by investigators for a House Government Operations subcommittee says, "To date, Intelpost has been a complete failure. Through the end of 1983, cumulative Intelpost revenues were $58,080. No zeroes have been omitted from this figure... A service that generated so little revenue must be considered a failure by any measure of performance."

Since 1978, development, testing, and operation of Intelpost have cost $6.2 million. This means the system has taken in less than one percent of its cost.

The House investigators were particularly exasperated at the Postal Service's lack of the most elementary records. It couldn't even tell them the number of messages that had been sent by Intelpost. The investigators wrote, "The committee is mystified that the Postal Service has not routinely compiled and made use of this basic management information."

The bottom line: the committee urges the board of governors to "terminate Intelpost as soon as practicable."

Victory for Wiretap Victims

The Associated Press

A $1.75 million settlement has tentatively been reached in a police wiretapping case involving more than 1000 plaintiffs and the city of New Haven, Connecticut [see "Wiretap City" in *2600*, March, 1984]. The settlement still needs the approval of two city boards and a Federal judge.

"This is a complete, 100 percent victory," said John Williams, the coordinating counsel for the 1,233 plaintiffs. He said the settlement provides each plaintiff with at least $1,000 and as much as $6,000.

Bank Records Aren't So Private

The New York Times

How much information should a bank divulge over the telephone about a customer's accounts? That question came up recently when a Manhattan real estate broker called a major bank's customer service number and, in less than two minutes, was told exactly how much a client had on deposit at a branch on the Upper West Side.

"That's information of the most confidential nature," said Gary Walker of the New York City Department of Consumer Affairs. "It shouldn't be given out without your permission, and probably not over the phone at all."

The bank the broker called, Citibank, says it does not routinely release detailed information about accounts by telephone and says it makes disclosures to outsiders only with the customer's written consent. In this particular case, Citibank said the customer service representative might have believed that the broker had the client's permission to obtain the balances.

But two weeks later, the same customer telephoned the bank and quickly obtained the balance in his checking account. The service representative asked when and where the customer had made his last deposit, saying the information was needed "for security reasons." As a test, the customer said he had deposited a check in the cash machine at Penn Station—Citibank has no machine there—and deliberately overstated the size of his last deposit. Despite the erroneous information, the bank's representative promptly told the customer how much money he had.

Norma Rollins, a lawyer with the New York Civil Liberties Union, said that one of her group's priorities for 1984 was a state law prohibiting unauthorized disclosures by banks. She said, "Banks can tell a pretty good story of your life—where you've been, what you've been spending. If you go to the corner liquor store every week to cash a check for spending money, think about what someone could say about your life style if they think you're spending $150 a week on booze."

June 1984

No More Free Info

2600 News Service

In a move that caught almost *everyone* off guard, AT&T quietly put an end to the age-old tradition of free directory assistance. As of the end of May, it now costs 50¢ for each call to long distance information (XXX-555-1212) within the United States. And unlike previous instances of local telephone companies charging for directory assistance, there is no way to avoid this by using a public phone! Information costs 50¢ from everywhere with these exceptions: local directory assistance, which is still controlled by the local companies and not AT&T; 800 & 900 info; Canadian info; and overseas info. AT&T is also generous enough to allow you two *free* calls to long distance info per month, providing you make at least two long distance calls per month. (No, other calls to information don't count as long distance calls!)

Reaction to this change ranged from total ignorance to complete disbelief. An AT&T operator told us, "We didn't even know about this until today! [the day it went into effect] I don't understand these people—they're going to lose a lot of customers by doing this. What they *should* do is charge only the people who aren't using AT&T as their primary carrier. Then we can advertise "free directory assistance" which no other company can."

As it happens, other companies such as Skyline now allow customers to dial long distance information on their networks. The calls are billed as if they were regular calls to that area. Since calls to directory assistance generally last less than thirty seconds, the charge winds up being less (sometimes significantly) than 50¢. If you choose this way to call information, you may be lucky enough to hear one of the info operators say, "Thank you for dialing AT&T." You can then have a good laugh at their expense.

Meanwhile, phone phreaks around the country were particularly indignant. "This puts a real crimp on silver boxing," one said. "And I'm sure our favorite corporations won't enjoy paying for our information calls now on top of all the other ones." Others have suggested ordering as many free telephone books as possible, and distributing them around the country or actually setting up an alternate directory assistance center. Free telephone books can usually be obtained through local phone companies.

2600 Writer Indicted

2600 News Service

It's been reported here and there that the editor of an underground magazine called *2600* has been charged with wire fraud in connection with the GTE Telemail investigation (see previous issues for details on this case).

One of our coordinating writers is, in fact, involved with this case—however he is not the "editor" of our magazine. *2600* is not handled by a single person, but by different people all over the country who contribute whatever they can according to their abilities.

We are not an "underground" magazine; we don't break laws or publish items that are illegal to publish. We simply discuss interesting things that can be done with today's technology. There is certainly no reason for us to go underground.

As for the investigation, we are confident that our writer will be vindicated and left alone. He is planning to write a story concerning this "adventure" when it's all over, regardless of how it ends. He has our full support and we hope he has yours as well.

Computer Threat Causes Chaos in Albany

Associated Press

Federal and local officials were baffled by a message which appeared on a computer terminal May 19 at Albany County Airport in Albany, New York. The message said that armed individuals would be boarding a plane, according to the FBI.

At about 7:15 am, the message was found on a computer screen at Boarding Gate 3. It warned that if anyone tried to interfere, "people would die." Security personnel searched a plane that was coming in at that gate, but found nothing.

The FBI and local authorities are trying to determine if the message was left by an airport employee or by an outsider who somehow broke into the computer system.

E-COM Is Going Away

Associated Press

The Board of Governors of the Postal Service has voted to get out of the computer mail business and possibly turn it over to a private contractor.

E-COM is what the Postal Service calls its computer mail operation, short for Electronic Computer Originated Mail. The system was designed for mass mailers, but never met its expectations since it began in January, 1982. The chief users of the system had been financial institutions, retailers, airlines, and hospitals.

AT&T Limits Use of Their Credit Cards

Combined News Sources

AT&T is in the process of barring direct-dial credit card calls from south Florida to 26 countries. The nations include most of Central and South America, some in the Caribbean and some in Asia, including Israel.

"The countries selected for the suspension of credit card calls are places to which a majority of international fraudulent calls are being made," said Barry Johnson, an AT&T spokesman.

The Israeli prime minister was unavailable for comment.

FCC Actions

Various Connections We Have

- The Federal Communications Commission has ruled that operators of the so-called "dial-a-porn" phone services must restrict children's access by limiting hours of operation to after the sun has gone down. Under the ruling, which goes into effect on July 12, tape-recorded messages will be restricted to between 9 pm and 8 am. Live services will still be available on a 24-hour basis, however. They usually require a credit card number.
- The FCC has voted to use a lottery to select three "network organizers" who would be responsible for constructing nationwide paging services. Such systems would allow a New York businessman traveling in California to be "beeped" by his home office (or anyone else who knew how to tap into the system).

The organizers will construct a long-distance transmission system using either satellite or telephone facilities to link local paging companies across the country. They will also oversee the use of one of the three special frequencies that have been set aside by the FCC to transmit the paging signals.

- Over the protests of MCI and GTE Sprint, the FCC has decided to allow AT&T to immediately begin a service that sets a flat monthly rate for an hour's worth of long-distance calls.

Under this new option, customers can pay $10 a month for an hour's worth of calling time each month for direct-dialed domestic calls placed during night rate periods. Wow.

July 1984

Look Out For Sidney!

Combined News Sources

The city of New York has come up with a new way to fight parking scofflaws. It's called SIDNEY—Summons Issuing Device for NEw York. It's a handheld computer terminal that will be able to get information about license plate numbers that are "suspected" of being attached to scofflaws.

The device weighs less than five pounds and looks rather like a calculator. It would ask whoever was operating it to enter the color, make, model, registration expiration, location, time, and nature of violation. SIDNEY would then print out a waterproof parking ticket and at the same time check its 10,000-plate memory to see if the license plate belonged to a scofflaw or a stolen car. An appropriate message would then be flashed on the screen. Details of each ticket issued would be stored in the device and entered automatically into the main computer system each day.

There hasn't been much talk circulating about what will happen when these things get stolen and fake tickets are handed out by the thousands. It is expected that these creatures will be turned loose into the hands of meter-maids within two years. The contract for producing SIDNEY has tentatively been awarded to Citisource of New Jersey.

Bell to AT&T: Get Lost!

Associated Press

One of the so-called "Baby Bells" is displaying its independence from its former parent—AT&T. Southwestern Bell says it's chosen GTE Sprint to provide long-distance telephone service for its Houston operation.

By using GTE Sprint instead of AT&T, Southwestern Bell figures to save about fifty thousand dollars. Long distance service from Houston currently costs the former Bell system unit about $300,000 a year.

GTE Sprint will replace AT&T in Houston in mid-August.

Five Arrested in Phone Fraud

The New York Times

Five Manhattan residents were arrested last month on charges of defrauding the New York Telephone Company by making more than 1,500 illegal telephone calls, mostly to the Dominican Republic, in a three-day period.

The Manhattan District Attorney's office said the suspects used "blue boxes" to make the calls. The five were charged with possession of burglary tools and theft of services. One was also charged with selling a stolen credit card number to an undercover investigator and using such numbers to make calls for other people. He could get four years for his trouble.

Supposedly, the suspects were offering neighbors low-cost long distance calls, however they frequently charged more than the cost of legitimate calls!

An Official Crackdown on Hackers

Combined News Sources

According to Rep. William Hughes (D-N.J.), computer crime is increasing by leaps and bounds. Speaking on the House floor, Hughes said, "It's time we recognized that computer 'hackers' who intrude into data banks are not just mischievous kids looking for fun. They're engaging in illegal activities which pose potentially serious threats to our society."

He urged quick passage of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, being sponsored by him and eight other House members, including Democrats and Republicans.

The House Judiciary Committee took a step towards making it a crime for hackers to break into systems such as TRW by adopting an amendment by Rep. Dan Glickman (D-Kan.). His proposal would make it a misdemeanor to raid computer files containing private credit histories or banking information.

A subcommittee staff lawyer said the bill would close loopholes in existing federal and state laws by making it a felony offense to access a computer without authorization and with intent to defraud, if that act enables the perpetrator to obtain anything worth at least $5,000 over a one-year period or any classified government information.

The bill is expected to come before the full House either late this month or in early August.

Pay Telephones Deregulated

2600 News Service

On June 15, the FCC decided to allow just about anybody to get involved in the pay phone business. Up until now, pay phones have been provided by whichever local company serves the area. But with this new ruling, all kinds of new companies will be seen. In fact, some phones may even have different prices! And, of course, it's to be expected that each of these new types of phones will have their own quirks and bugs. Look for Matrix, Tonka, and Paytel phones in the near future.

Of course, there will be disadvantages. Some phones will only be able to dial locally. Others won't be able to reach 911 or information. Many will probably be rotary and most will certainly break down more frequently. Still, diversity is what makes this entire field so interesting.

"You Must First Dial a One..."

Associated Press

As of July 1st, 3 million customers in New Jersey had to start dialing a one before area codes when calling long distance. This leaves 202 and 516 as the last remaining areas in the country that don't have to do this.

Company officials say the new system was introduced to provide 152 more exchanges to meet increasing customer demand. Under the new system, New Jersey Bell will begin using certain area codes as telephone exchanges. They will avoid using area codes of neighboring states to prevent mass confusion.

Information News

Combined News Sources

Starting this month, MCI will connect subscribers to long distance information just like AT&T does. And, like AT&T, MCI will offer two free information calls per month, provided their service is used for at least two long distance calls in that same month. After that, they will charge for a call to information, just like AT&T does! So what's the difference? In the price, of course. AT&T charges a hefty fifty cents for each call to directory assistance, while MCI will be under-selling them with an affordable 45¢. Good old capitalism.

In another development, a computer program to help find a telephone number without complete information from the caller has been patented by Richard H. Boivie for Bell Labs. In cases where the caller can give the information operator the name of the person being sought, but is unsure about the spelling, the computer will trace alternative spellings. It will also sort through different addresses for the most likely candidates.

August 1984

Big Brother No Longer Watching Miami

Associated Press

City officials who stirred up visions of George Orwell's "Big Brother" when they installed video cameras to detect street crime have decided the project wasn't such a good idea after all.

So three years and almost $300,000 later, the city has abandoned its "Television Police Protection" system, saying it failed to record one crime.

The city had the cameras installed in February 1982 but for numerous technical reasons the system wasn't turned on until that June.

The project called for 20 cameras to be mounted on a rotating basis in 100 camera housings mounted on poles, thus keeping criminals off guard.

Another larger camera was mounted atop a 14-story building on Lincoln Road to sweep the length of both streets for a broad overview.

But the system had trouble. "We had continual maintenance problems with constant adjustment of the microwave," Police Chief Kenneth Glassman said. One civilian made so much fuss about police watching the monitors and not patrolling the streets that the department took police off the project. Another problem was in lack of interest from civilian volunteers assigned to watch the monitors. Many times, even the few working monitors went unwatched.

Computers Seized as Summer Games Begin

Long Island Newsday

The home computers of four Huntsville, Alabama teenagers were seized by the FBI last month after an illegal tap into NASA computers. The unauthorized taps, according to the FBI, destroyed records and blocked scientists from using the computers. The FBI seized computers, printers, floppy disks, and software that allegedly were used to tap into two computers at NASA's Marshall Space Flight Center. They contained no classified information, according to NASA officials.

Cecil Moses, special agent in charge of the FBI's Birmingham office, said an investigation is continuing. He said no charges have been filed, but may be later.

House: Hacking is Bad

Combined News Sources

The House of Representatives has voted 395-0 for a bill that would make it a federal crime to gain access to computer memory banks without permission. The legislation would combine the attack on hackers with an attempt to stop those who manufacture or possess fraudulent credit cards or use someone's credit card number without his or her knowledge.

More PC Jr's., Less Z-100's for Soviets

The New York Times

The United States, 13 NATO allies and Japan have jointly agreed to impose broad, new export controls on the sale of small computers and sophisticated telephone equipment to nations of the Soviet bloc. The agreement comes after two and a half years of difficult negotiations.

The accord, which was reached at the urging of the U.S., expands the existing NATO embargo on the sale of large sophisticated computers to include smaller models that could have military applications. This means that many of the more expensive personal computers now available at retail outlets in the United States will be subject to export controls in the future.

Also, the agreement sets maximum levels of technological sophistication for digital switching and other telephone equipment supplied to the Eastern bloc by Western corporations.

The Reagan Administration took the most restrictive line throughout the embargo review talks, diplomats say, with the Europeans and Japanese advocating a more liberal approach to trade with the Communist world. The U.S., though, did agree to liberalize the sale of some less advanced computers to the Eastern bloc countries in return for joint Western restrictions on the sale of certain powerful small computers.

In addition, the Western powers have undertaken to ban the export of "ruggedized" computers, built to withstand rough treatment and thus suitable for battlefield use.

Federal Express Offers "E-Mail"

Time

Memphis-based Federal Express, which pioneered next-day private postal service, is now promising even greater speed with ZapMail, its long-awaited version of electronic mail. For as little as $25 for a missive of five pages or less and up to $50 for a maximum of 20 pages, Federal Express will zap letters and documents across the U.S. within two hours. Unlike other outfits, Federal Express does not require its customers to use computer keyboards to enter messages. Instead a courier comes and picks it up, takes it to a Federal Express office, where clerks feed it into a document scanner for transmission over land lines. At the receiving Federal Express office, a laser printer will spew out copies for couriers to deliver immediately. [No, this is not electronic mail in the bona fide sense.] The firm even vows to give full refunds if documents are late.

ITT Wiping Out Fee

Associated Press

On September 1, ITT will drop the monthly service fee it charges users of its long-distance telephone service. The fees currently are $5 a month for residential customers and $10 a month for business users. ITT also said it would introduce discounts for high-volume callers, and said its residential customers would be able to reach any telephone in the continental United States. Previously, only ITT's business customers had nationwide calling. ITT is ranked eighth among long-distance carriers with about 125,000 customers.

800 Directories Now Available

A Friendly Information Operator

Starting in the middle of September, AT&T will at last start offering directories to toll-free numbers. Previously, the only way to get such a directory was through scanning, trashing, or buying a directory printed by an outside company. There are two versions being offered. One is for people and sells for $6.25 while the other is for businesses and sells for $8.75. Info can be had by calling 8002424634. If that doesn't work from your area, call 8005551212 and demand an explanation. Billing won't be done through your phone bill, as one might expect. "We don't have *that* kind of capability yet," they said to us.

Ice Cream Chain Aides Selective Service

The New York Times

The Selective Service System has defended its use of a mailing list compiled by a national chain of ice cream stores to advise young men that they were liable for draft registration.

However, the government will be returning the computerized list of 167,000 names to the company.

Alexander Hehmeyer, executive vice president and general counsel of Farrell's Ice Cream Parlor Restaurant, a chain of almost 100 ice cream stores, said both he and the company were "upset and outraged" by this "act of big brother government."

For many years the retail outlets of Farrell's have had customers fill out a birthday form so that they would get birthday cards from the company entitling them to free ice cream sundaes. The Selective Service bought the Farrell's list in 1983 from a list broker in New Jersey. Last October, the system began using the list to mail 1,500 to 3,500 warning cards a month to young men whose listed birthdays indicated they were about to turn 18.

Besides commercial lists, the Selective Service relies on state agencies that license drivers and the Defense Department, which compiles a list of high school graduates.

September 1984

NSA Doesn't Feel Secure

The New York Times

The National Security Agency has told Congress that United States advantages in advanced technologies, including development of nuclear weapons, are threatened by the poor security of the nation's communications networks.

To protect information, the agency recommended that a single agency supervise the development of communication security procedures, the purchasing of telecommunications security equipment and carrying out personnel security procedures.

The National Security Agency is the largest and most secretive of the nation's intelligence agencies. Its chief responsibilities are to collect intelligence by eavesdropping on the electronic communications of other nations and to devise ways to prevent foreign countries from acquiring the confidential messages of the Defense Department and other security agencies.

Jerry F. Berman, legislative counsel to the American Civil Liberties Union, agreed that the swift development of computerized communications systems had made security a legitimate public concern.

"But what is disturbing about the proposal is that it comes from the N.S.A., a super-secret agency with a major foreign intelligence mission and the least accountability of any agency in the United States Government," Berman said.

"If any agency is competent, it is the N.S.A. The problem, however, is that they are not accountable and cannot be counted upon to weigh other interests, such as the privacy of all American citizens.

"If the N.S.A. were to get involved in procurement, for example," Berman added, "they could end up putting a net of security over large parts of the academic community and industry. It might increase security, but it also could reduce freedom and hinder the open development of new forms of communications."

A list was not provided of the Government telecommunications networks that might come under the overall control of a centralized security agency if it was given a broadened mandate. The Federal Bureau of Investigation, the General Services Administration, and the Federal Reserve operate national communication networks that would qualify as being among "the nation's automated information systems."

Another Hacker Story

Associated Press

A boy who allegedly bought rare comic books and other goods worth thousands of dollars by using a computer to get credit-card numbers is helping authorities trace other hackers across the country, Howard County [MD] police say.

He has cooperated with local police, FBI, and Secret Service investigators by providing information about illegal computer operating practices. The youth allegedly bought computer equipment and programs valued up to $4,000 by using credit card numbers supplied by computer hackers from the Midwest. He ordered the goods by telephone and then picked them up after their delivery to unoccupied homes.

Police obtained a warrant to search the boy's house August 16 after talking with an informant. Found were programs that allowed him to patch into several long distance telephone companies illegally. Police say he apparently was able to call around the world and arrange conference calls using corporate telephone lines.

[Must have been a real genius...]

AT&T Faces Serious Money Problem

Associated Press again

The American Telephone and Telegraph Company, despite service backlogs and increased competition, has moved closer in recent months to its maximum authorized profit margin for interstate long-distance telephone service.

A company spokesman said late last month that AT&T's rate or return, or profit margin, on long distance service was 12.36 percent after the first seven months of 1984. The maximum authorized margin is 12.75 percent annually, based on AT&T's investment in equipment.

Among long distance companies, only AT&T faces an Federal Communications Commission limit on profits. The commission last adjusted the margin in 1981 after more than a year of study, raising it from 11 percent. Should AT&T exceed it's margin, the F.C.C. can order rate cuts.

Private Directories Soon to be Available

The New York Times

How valuable are the telephone directories of some of the nation's top banks, investment and accounting firms, insurance companies, and corporations—especially those that include not only direct office numbers for managers, but also home addresses and phone numbers and, in at least one instance, such data for summer homes?

Steven Olsen is counting on their being worth a great deal. His firm, Corporate Information Services, plans to sell copies of directories for such companies as the General Motors Corporation; the RCA Corporation; Chase Manhattan Bank; Goldman, Sachs & Company; Arthur Andersen & Company, and Booz, Allen & Hamilton, the management consulting firm.

Prospective buyers are told to write to a box number and ask for a catalog detailing what Mr. Olsen said would be a package of directories for 250 companies from around the world. They must then submit bids through the mail for his package. Bidders topping a minimum set by Mr. Olsen's company would receive the package, and, he said, "we're not talking small money. This is a valuable source of information to stockbrokers, executive recruiters, [computer hackers,] insurance and real estate brokers, and those engaged in direct-mail marketing or telemarketing. We're talking about the most powerful companies and some of the highest-salaried people in the world," he added.

Mr. Olsen, who said he got his idea while working as an editor for a computer publication [it wasn't us, we *swear*], showed off copies of in-house directories for Chase Manhattan and Goldman, Sachs during an interview. His plans drew a cool response from both companies.

Many other companies declined comment on the attempted sale of their directory information. The reaction among those that did ranged from outrage to hearty amusement.

"We only have copies of the directories," Mr. Olsen stressed, not the directories themselves. "So we're not in receipt of stolen properties, and I acquired them all legally."

But Mr. Olsen, who wants to sell other people's addresses and telephone numbers, declined for "reasons of security" to disclose the address or telephone number of his company. There was no listing for Corporate Information Services in telephone information for New York City, and the address to which inquiries about the auction are to be sent is a mailbox in a private postal drop company on lower Fifth Avenue. Mr. Olsen was reached through an answering service, whose number is not as closely guarded. [The folks at *2600* would be more than proud if some of our readers were able to find out this guy's phone number so we can display it on *Page One!!!*]

Mr. Olsen said that such secrecy was necessary "as protection against attempts to steal or destroy this valuable database." He said he was followed for a time and "had to take evasive action" last year after a newspaper published an article about the company.

Mr. Olsen also said that he had no copies of company directories that are copyrighted. Victor A. Kovner, a lawyer who is a copyright expert, said that if a company has copyrighted its directory and given notice in it, the book cannot be reproduced without permission.

Mr. Kovner said that if a company has not copyrighted its directory, then in most cases it could not prevent copies from being disseminated.

[To illustrate this point, we have published a picture of a directory that is not copyrighted. We suggest you look at it so you'll understand this article better. And as a public service to nearly everyone, we challenge Mr. Olsen to beat *our* price for "public" information, which is simply the cost of xeroxing and mailing it. We'll cheerily make available *any* documents (non-copyrighted, of course!) provided by contributors for a no-profit price. So send them on in!]

October 1984

NSA Wants Better Phones

The New York Times

The National Security Agency is proposing that the Government and industry be equipped with as many as 500,000 telephones that can be secured against interception.

The agency is convinced that the Soviet Union and the other nations are obtaining important intelligence from United States telephones.

Although cloaked in secrecy, a program like the one the agency proposes could cost hundreds of millions of dollars. Under the proposal, production of the secure phones would begin in two years.

The number of secure telephones currently used by Government agencies is classified information. But the Carter Administration said there were 100 such phones in the Government and it planned to buy 150 more. The cost of each phone then was $35,000. The Reagan Administration has bought an unknown number of additional secure phones.

"Anyone making a phone call to the West Coast or Boston from the Washington area has no idea how the conversation will be transmitted," an NSA spokesperson said. "It might go via fiber optics, conventional cable, microwave towers or one of the 19 domestic satellites. If it is going via satellite you can presume the other guy is listening to it."

Oh No, Not Again!

Associated Press

The House passed a bill on September 17 by voice vote that would make it a Federal crime to gain unauthorized access to or tamper with computerized medical records.

Victimized by Crime Computers

The New York Times

Police officers went to an apartment in New Orleans looking for a woman named Vera Davis, who was wanted for theft and forgery. Although the woman who answered the door identified herself as Shirley Jones, they arrested her anyway. A police computer listed Shirley Jones as an alias used by the forgery suspect. That was two and a half years ago.

According to her attorney, Mrs. Jones, who was once advised by a sheriff's deputy to change her name to avoid future arrests, is one of a growing number of people in New Orleans who have gotten in trouble with the law because of inaccurate, outdated, or misused information in police computers.

The New Orleans computers are part of a national network. From a local terminal, a computer check can be run through the National Crime Information Center in Washington, operated by the FBI, in less than a minute.

The New Orleans case, said Robert Ellis Smith, publisher of *Privacy Journal*, a newsletter that reports on privacy cases from Washington, DC, is "symbolic of a larger national problem, an incredibly high rate of inaccuracy" in criminal records and "an inordinate amount of mistaken identity cases in the criminal justice information systems."

Sears Satellite Network

Associated Press

The American Satellite Company has signed a contract with Sears, Roebuck and Company to construct and operate a private communications system linking corporate offices of Sears and its subsidiaries in 26 United States cities. This would be the largest private system ever developed capable of offering full-motion video teleconferencing.

Loopholes Around Wiretap Laws

The New York Times (again)

Senator Patrick J. Leahy, Democrat of Vermont, has said that he will seek legislation to improve protection of privacy by closing gaps in Federal wiretapping laws.

He and several experts said at a Senate Judiciary subcommittee hearing that it was unclear, for example, whether existing laws permitted Government officials or others to intercept electronic mail, or even ordinary telephone calls sent by computer or microwave technology, without a warrant.

"There are tremendous holes in communications privacy today," testified Ronald L. Plesser, a Washington lawyer who has long specialized in information privacy issues.

The experts at this hearing testified that private interception of electronic mail and other messages carried through telephone networks may not violate Federal law.

IBM is Buying Rolm!

The New York Times (yet again)

IBM has said that it will buy the Rolm Corporation, in a move that will heighten the competition between the world's largest computer company and AT&T. The price? $1.25 billion.

"IBM wants it all, it needs it all," said Esther Dyson, editor of Release 1.0, an industry newsletter. "They have a biological urge to grow."

Most analysts, however, said that IBM had realized—perhaps belatedly—that it greatly needs to strengthen its offerings in telecommunications switching equipment.

Rolm, founded in 1969 as a maker of military computers is now a leading maker of private branch exchanges, systems that control both voice and data communications over the telephone.

911 Suspect Hung Up

The New York Post

A notorious hoax caller who has plagued 911 switchboards for three years has been nabbed reporting another bogus crime, police say.

Cops say the suspect—who they have been unable to identify—made more than 500 false reports ranging from strangulations in progress to rapes and shootings of police officers.

He was arrested at a Penn Station pay phone while telling a 911 operator he had just raped and strangled his girlfriend with her pantyhose. That was the fabricated crime he reported most frequently, according to police.

"He called every day of the week at all hours," said Sgt. Stephen McDonald.

"He was causing a lot of problems and the 911 people were really looking for him," said Officer James Lapiedra who collared the hoaxer.

According to McDonald, news of the hoaxer's capture was jubilantly received by 911 operators: "There was a lot of cheering."

In the words of Lapiedra, "He was surprised he was caught."

November 1984

Computer Foul-ups Hurt Social Security

The New York Times

A House Committee has asserted that improper handling of a $115 million computer contract had undermined the Government's ability to serve the millions of Americans who receive Social Security benefits.

The report that improprieties in the 1981 selection of the Paradyne Corporation, a Florida company, to build computer terminals had damaged the daily operations of the Social Security Administration came from the House Government Operations Committee, after two years of investigation.

After Paradyne provided the terminals, field offices of the Social Security Administration experienced "extraordinary levels of equipment failures and poor performance," according to researchers.

The report cited complaints from local Social Security offices all over the country. "The public is frustrated with us and we're frustrated with the system and snapping at each other," wrote the Fayetteville, NC manager on July 9, 1982. "Something has to be done immediately. The public will be after us with guns and knives shortly."

Phones in the Sky

2600 News Service

Last month, six airlines began a pay-telephone service that allows passengers to call anywhere in the United States. The cost is fairly phenomenal: $7.50 for the first three minutes and $1.25 for each additional minute.

The system (designed by Airfone Incorporated) uses radio waves to transmit calls to one of 37 ground receiving stations, which then transfer them to regular telephone lines.

To use the system, you insert any one of seven major credit cards into a wall-mounted console situated in the front of the plane. When the card has been validated, a cordless phone will be released, and you can return to your seat to dial away.

Another FBI Computer File

The New York Times

An advisory panel of the Federal Bureau of Investigation has approved the testing of a computerized file that could allow criminal justice agencies all over the country to exchange the names of white-collar crime suspects and their associates.

An FBI staff paper presented to the panel said the file, the Economic Crime Index, would permit a "more efficient and effective field-wide coordination of major white-collar crime investigations, particularly those involving financial crimes."

Civil liberties experts, however, immediately challenged the project, contending that the widespread exchange of "raw investigative files" would be a dangerous threat to innocent Americans. They said that such networks should be limited to handling public information such as a person's arrest record.

The information would include the names of suspects, their addresses, Social Security numbers, passport numbers, bank account numbers, aliases, Selective Service numbers, driver's license numbers, automobile license numbers, and information about "associates."

According to Jerry Berman, legislative counsel of the American Civil Liberties Union, the project "is extraordinarily troublesome, because it is not intended to exchange public record information such as when someone is arrested or when an arrest warrant has been obtained for someone who is believed to have committed a crime. Instead, the FBI will be passing around information that will include many unproven allegations and casual gossip, the dissemination of which presents a major threat to the privacy of all Americans."

Berman noted that information available on the proposal did not define what was meant by white-collar crime or "an associate." He said, "An associate of a white-collar criminal might be a casual friend you met at a party or, in the case of a suspected bank officer, all the members of the bank's board of governors."

Use of Wiretaps at Record Pace

Long Island Newsday

The use of wiretaps by federal law-enforcement agencies has been steadily increasing, with a record number expected this year as the FBI becomes more involved with narcotics investigations, according to Justice Department sources.

American University law professor Herman Schwartz, who monitors the use of surveillance, thinks there are not enough safeguards in the use of wiretaps. "I think there is an enormous intrusion into people's privacy," he said, citing recent FBI public-corruption probes. "Now they are reaching into the lives of a number of innocent people because of the types of crimes they are going after," he said.

For each wiretap installed, an average of 1,107 conversations were overheard involving 147 persons, according to the 1983 court report. In that year, the cost of installing federal wiretaps averaged $65,000 each, for a total cost of more than $13 million. But critics claim that figure is too low because it doesn't calculate the legal work involved. All wiretaps have to be court-authorized.

The rapid increase in the number of wiretaps, which sources said already has topped last year's total of 208, probably will surpass the 1971 record (285) set by the Nixon administration. Use of wiretaps dropped soon after President Jimmy Carter took office, with an all-time low set in 1977. The use of electronic surveillance started to climb again in 1981 after President Ronald Reagan took office.

818 Here to Stay

Combined News Sources

After three years of warnings and nine months of what the telephone companies called a "permissive dialing period," 1.5 million Los Angeles area residents have been split off from 3.7 million neighbors as the area received its first new dialing code in nearly 40 years.

Callers to downtown Los Angeles, Beverly Hills, Hollywood, and the trendy beach communities of Malibu and Santa Monica can continue to use the old 213 code. But anyone calling San Fernando Valley and the suburban San Gabriel Valley now have to dial 818.

Alfred Kness, a computer equipment salesman who was making rounds through the downtown area, pulled out a thick booklet full of clients' business cards and said, "It's so exciting now. I never know who I'm going to reach on the first try—a customer or that nice mechanical lady from the phone company. It stinks."

One We Somehow Missed

A Local Paper in Upstate New York

JANUARY 27, 1984—Two 18-year-old Stony Point (New York) "rustlers" have been named as the outlaws who lassoed a Letchworth telephone booth to their car and dragged it two miles through the dust before being arrested by state troopers. Both of the accused were charged with grand larceny, possession of burglar tools, and criminal mischief.

A witness reported seeing two men tie up the outdoor booth at about 3:35 a.m., pull it from its moorings in a concrete slab and drag it along the highway. "They were tracked by following the scratch marks on the highway," a state policeman said.

The troopers found the booth a good two miles from its point of origin. A security officer from the New York Telephone Company said the booth cost $1,385, the coin machine $400, the wire that led out of it another $46, and the concrete-slab it was pulled from was worth another $278. He said the machine, with an estimated $50 in change still in the coin box, was "totaled".

"We're going to be looking for restitution," the company representative said.

In Addition...

Combined News Sources

- Attorney Melvin Belli has filed suit in Santa Ana, CA against TRW Inc., accusing the nation's largest credit rating firm of "dangerous and unethical" practices that exposed credit histories to computer pirates. This is the first of many similar lawsuits Belli intends to file nationwide.
- MCI says its customers now can call Belgium, Argentina, Brazil, East Germany, Greece, and the United Arab Emirates. (Presumably, the MCI trademark, i.e. LOUD echoes, will continue to flourish with this expansion.) MCI has negotiated agreements that will allow the start of direct overseas phone service next year to England and three other (as of yet unnamed) foreign nations.
- New York's chief judge has proposed having a computer help select guardians and conservators in an effort to combat the appearance that appointments may be handed out as political favors. Under the system, each time a judge needed to make an appointment, the computer would randomly select five names from which he could choose. The chief judge would establish statewide standards for placement of names on the lists. Hackers, though, would probably bypass these standards.

December 1984

Computer Makes It Easy for Reagan

The Associated Press

Using $1.1 million in research money from the Republican National Committee, a team of 26 computer operators and analysts, who called themselves the Opposition Research Group, scrutinized every available aspect of Walter Mondale's political career.

The team collected uncounted hours of videotape and 75,000 quotations, coded, cross-referenced, and entered in a giant computer at the Republican headquarters on Capitol Hill.

"Walter Mondale couldn't open his mouth without our analyzing it in 45 seconds and determining whether he was telling the truth," Michael Bayer, director of the team, said. "It took them days to monitor the same thing that we were cranking out."

Beginning in April, every speech text, every television appearance, every vote Mondale had cast in his political career was broken down, analyzed, coded by category and entered in the electronic file. While Senator Gary Hart was still in the race for the Democratic nomination, his record was scrutinized as well. And after Mondale chose Geraldine Ferraro as his running mate, the team made the study of her life a priority project.

They used the information to insert attack lines into Reagan speeches. And Vice President Bush's staff aboard Air Force Two could plug directly into the team's computer to check things Mr. Mondale had just said and counter with new charges of their own.

Penetrating the Pentagon by Phone

The New York Times

The Pentagon employs 25,000 people, who work, in one way or another, on national defense. But to many outsiders who have tried to reach someone at the huge office building, the Pentagon's best defense is against incoming phone calls. That situation is about to come to a halt, according to the Lockheed Electronics Company, which has installed a computerized directory assistance system at the Pentagon on an eight-year contract worth $1 million. Now an operator can find a number even if the caller lacks such information as the party's first name or office location. The new system has about 150,000 listings. The number to call is 2025456700.

First of the "Superminis"

Los Angeles Times

Digital Equipment Corporation has unveiled its new "supermini" computer, the powerful VAX 8600, which starts in price at $576,000. This machine, produced under the code name of Venus, can compute at a speed more than four times that of DEC's previous computer. With full peripherals, the 8600 will cost almost a million dollars. They should start popping up all over the place in April.

Students Bog Down Computer

The Associated Press

Some students at Ohio's Oberlin College don't like the fact that their school has investments in South Africa. So to protest that fact, they tried to overload Oberlin's main computer and another in the school's library on November 30. At the same time, more than 200 students staged a silent demonstration outside a meeting of the Oberlin College Board of Trustees. The trustees took no action on the matter.

SBS Offers Toll-Free Service

2600 News Service

SBS Skyline recently came up with an alternative to the standard AT&T in-WATS service which could become quite popular. It works as follows: In many parts of the country, SBS Skyline can be accessed toll-free by dialing 950-1088. To make a toll-free call on Skyline, the caller would first access the system, using the number above. Then they would enter a six digit "service code" which would ring whatever phone number has been assigned to that code. The result is the same as making an 800 call, but the procedure is different. For instance, the caller *must* be at a touch-tone® phone to enter the service code. The caller must also know in advance what this six digit code is. And Skyline service still isn't available all over the country. But this system is much easier for the called party. While an 800 line can cost hundreds of dollars to install, Skyline only requires a $15 monthly minimum per line.

Electronic Jail All Screwed Up

The New York Times

Travis County (Texas) officials had hoped to open their new $12 million jail with its advanced electronic locking system last year.

Unfortunately, the jail is still not open. Or rather, it's too open.

"In 1983 we were supposed to move in, and we discovered the locking mechanisms were not adequate," Sheriff Doyne Bailey of Travis County explained.

"Not adequate" may understate the problems, which Mr. Bailey says relate to an "inherent design problem that allows the locking system to be defeated."

The locking system is integrated with other security equipment, so that locking a cell door will turn on an intercom. Or turning on an intercom will unlock a cell.

And when a fire alarm goes off, officials reported recently to the Texas Commission on Jail Standards, all the cells unlock.

That particular feature, they noted, may not be wholly desirable.

Video Telephone Invention

The New York Times

A new two-way video phone that makes use of any single standard telephone line has been patented by Jerome H. Lemelson, a prolific inventor with more than 350 other patents, and Christian Grund, a research scientist at the University of Wisconsin.

According to the patent, the new video phone functions without any interruption of conversation by transmission of pictures or data. A portable, self-contained unit can be provided at each end of a conventional telephone circuit. Each unit has a television camera and a display screen. A speaker and microphone may be carried within the housing or in a telephone handset. A picture printer may also be provided to record the images on the display screen.

Federal Telephone System Upgrade

On Communications

In what has been called the largest telecommunications buy in history, the U.S. government is spending more than a billion dollars to modernize its massive Federal Telephone System (FTS). This huge upgrade includes 1.3 million telephones, 15,000 trunk circuits, and 1,655 private branch exchanges (PBX).

According to Dr. Bernard J. Bennington (BJB), the General Services Administration (GSA) administrator in charge of the buy, the FTS is only slightly smaller than a Bell operating company and five to six times the size of the General Motors (GM) telephone network [see "Exploring Caves in Travelnet"].

At the present, the FTS is largely a voice system. About 15% of the network, however, consists of facilities for data transmission. Although the data portion sounds like an insignificant figure, it represents as much data as is moved in all the other civil agency networks combined.

Basically, the main justification for the system itself and the continuous battle to keep it upgraded is to provide continuity of government. Until the '60s in general, and the April 1961 Bay of Pigs situation in particular, there was a large comfort index surrounding the nation's telephone system. Until that time, it had been tried and always found adequate.

"During the Bay of Pigs operation, no one could get a phone call in or out of Washington," BJB said. "Naturally, we must have a viable, up-to-date communications system to support our national defense. And it must operate cost-effectively," he continued. "We cannot mix military and civil agency traffic."

LETTERS

We got our first letter to the editor in our second issue (February), which is really the quickest we could have possibly gotten one. Still, it took a while for what eventually became our all-time most popular feature to catch on. The next letters weren't printed until June and from that point they appeared every month. During our newsletter phase of 1984-1986, letters were confined to a single page or less. Who knew back then how much they would grow afterwards?

February 1984

Q&A

Got a question for us? Write it down and send it to us! We'll do our best to come up with an answer. Send it along to:

2600
Box 752
Middle Island, NY 11953

Q. How does the operator find out if you are calling from a fone booth or a house fone? Is there any way to defeat this?
—California

A. A pay phone is wired up directly to the TSPS (Traffic Service Position System, basically the operator at a switchboard) circuit. A light on the console flashes and shows the caller to be at a pay phone. To convince the TSPS that it wasn't actually a pay phone, you would have to go into the switch room and rewire it. The distinction is not made within the phone itself, but in the central office. You receive a dial tone through the TSPS circuit before it goes to the central office—it's connected in series with it. Everything you do goes through the TSPS circuit, whether it's local or not. In short, there's no way around it.

2600 needs writers! This could be your big chance!! If you come up with something to contribute, send it in to the address at the end of Q & A. Please send us your comments and criticisms as well. And spread the word! 2600 is bringing the good word of hackers and phreakers throughout the land of disks and relays!

June 1984

LETTERS FROM OUR READERS

5/28/84

Dear *2600*:

This is Quasi Moto, SysOp of the late Plover-Net Bulletin Board System (BBS). I am writing this letter to try to explain to all of you just what really happened to Plover-Net.

I guess the main reason that I took the system down was that I could only take so much of all of it. What exactly do I mean by "all of it"? Well, first and foremost, it's not easy going to bed every night thinking, "Will the Feds call tonight? Will my BBS be crashed by some hacker with nothing better to do?" and so forth. And then I awaken at 4:40 am to the annoying sound of the Rana recalibrating. Since I'm up, might as well validate users, etc. I notice that "?Syntax Error" is on the board, yawn and snicker as I smash the RESET key and the modem gives a sharp click as it disconnects that loser from the BBS.

The BBS re-runs itself and I logon. The first new user is "Fuck You" from "Your, asshole". 3 users later it's "Rachal Amato" (the name CN/A has for the BBS line). And then there are 2 messages with I/O errors in them which I must delete, despite the fact that the Rana is full at 202 messages and I must delete the first 5-10 (which takes on the order of 5-10 minutes). Then I get to take a shower and get dressed before school!

But I guess the real reason I took Plover-Net down was money. The phone bill, on the order of $50 or more a month was defrayed by about $15-20 per month. Which left me with about $30 every month to pay *from my own pocket!* This doesn't even touch the electricity it draws or all the software updates. That is when I put a stop to it.

I would like to stress the point that Plover-Net was *not*, I repeat, *not* busted, or for that matter, ever contacted by any law enforcement agency. I took it down of my own free will. I would like to take this final opportunity to give a piece of advice to all you other phreak SysOps...stay cool and put up my disclaimer. It's the "perfect" disclaimer. If you need a copy, or need to get in touch with me urgently, write to Quasi Moto c/o 2600 Magazine.

Dear *2600*:

Your article on step switching was super informative. Now I have a question. I found a really strange telephone switching center. It's 518-789. Can you tell me what type it is? It is so strange when you call it you can hear it dialing the number. And it starts ringing and you can still hear it dialing! It is crazy! What is it?

Awfully Curious

Dear AC:

518-789 is a very, very small (XY) step by step switching center. And if it's like most of them, it could be in a trailer or a very small building. It could even be in a house where the owners can keep a close tab on it. A test number for this exchange is 5187893299.

The dialing sound you described is fairly common with step offices. We're dealing with an independent phone company toll center here—it only does what it's told to do. The toll switcher is dialing a complete 7 digit number. Now, Western Electric doesn't allow you to hear pulses. When you dial into a step, though, different rules sometimes apply. If, for example, you dial 5187892000, it will immediately start ringing after the 7892 because there is no 7892 group. But it will dial the three zeroes after the two anyway, and you can hear that on top of the ring. *(If you have a question about a particular telephone exchange or a comment about phones and/or computers, send it to us at: 2600, Box 752, Middle Island, NY 11953. Anonymous letters accepted cheerfully!)*

July 1984

LETTERS FROM OUR READERS

6/14/84

Dear *2600*:

A few exchanges in my vicinity have recently upgraded their switching equipment. On 11/5/83, 914-268 switched from a SxS to a Northern Telecom DMS100. 914-634 & 638 also switched from a No. 5 Crossbar to a DMS100 on 6/9/84.

Through trashing, 99XX scanning, and "social engineering," I have found out the following: The suffix -9901 is a "verification" recording. In 268: 9903, 9906, 9909, 9911, 9912, & 9913 are all various recordings.

Another neat function on DMS100 is that you can hear the MF tones after most calls. NYTelco calls this the sound of their new system helping to serve you better.

Also, these CO's are under NYTelco jurisdiction. Yet, they bought from Northern Telecom DMS100 instead of a "nice" ESS system from Western Electric. Could this be the break-up at work?

This equipment offers ESS functions such as call waiting, call forwarding, dial-tone-first fortresses, etc. My question is: What type of toll-fraud equipment is standard or optional for the DMS100? Does it record everything like a pen register? Etc...

Curious

Dear Curious:

First off, our compliments on your ability to notice the changes that most people miss. As far as your 9901 discovery, many exchanges in your area have been known to do that. If you dial XXX-9901, you'll hear a computer read the exchange and area code. It doesn't really serve much of a purpose. But interesting things can always be found in the 99XX area, if your company uses it.

Concerning the DMS100, it is the break-up of the Bell System to an extent. New York Telephone has been buying equipment from Northern Telecom for some time now. But since the divestiture, they've become a little more flagrant about it. You'll see quite a bit more experimentation with products from other suppliers in the near future. The DMS100 is a very good switch, but it's got certain drawbacks as far as phone phreaking is concerned. It does have certain "devices". These don't work *exactly* like a pen register, but they wind up having the same effect. What is done is this: if you happen to send a 2600 Hertz tone down the line, DMS100 will make a computer record of whatever you did in the surrounding time. They automatically investigate your line if this is detected more than an undetermined amount of times. This is where the pen register comes in. The system is already equipped to handle a pen register through a special box in the exchange that's set up entirely for that purpose. This box ties into their automatic surveillance equipment. So it's kind of a two step process, but the DMS100 makes it much easier.

So far, we haven't been able to find any advantages (or bugs) in a DMS100. We will continue to look, though. Regarding the MF tones, they're simply not being filtered as they are in most places. The GTD#5 (made by GTE) and the DMS100 both, as a rule, only filter about ten percent of the MF tones. They also don't filter out rotary outpulses, whenever they exist. Perhaps it's a way of cutting corners.

DMS100, as you know, sounds just like ESS. About the only way you can tell if you've dialed into one is if you hear absolutely no clicks or pops when the party answers, as you do with ESS, crossbar, and step. Instead you hear a real faint, mild tick. When dialing out on one, you won't hear any clicks either.

Dear *2600*:

I hear you people are keen on answering people's questions, so answer me this: What ever happened to that operator who was so damn nasty that she refused to call that ambulance for this guy's dying mother just because he used a couple of cuz words on the telephone? By the way, the lady died a horrible violent death, I think. (I think the operator didn't die yet.) Oh yea, I also think that there was some sorta lawsuit against the nasty-oppy or the telco or someone.

RC

Dear RC:

The incident you're referring to took place a few months ago. It happened in Dallas, Texas and it concerned a man who was trying to get an ambulance for his mother-in-law who was having a massive heart attack. Not only did the operator refuse to send an ambulance until the woman herself got on the phone, but her supervisor *also* got on the line and said something to the effect of, "Sir, if you don't quit cussing out the operator, I'm going to have to hang up on you."

The operator was fired and the supervisor demoted. But both are currently claiming that they were only following orders. The city of Dallas allegedly said that at all costs an ambulance shouldn't be sent out unless it was an extremely life threatening situation. Anonymous people have even come forward and claimed that bonuses were offered to those who sent the least amount of ambulances out!

We should say that this doesn't involve the phone company, since it wasn't their operators who handled this call. Any lawsuits would be against the city of Dallas, in all likelihood. It's also interesting to note that there is no 911 service in Dallas. Residents there dial 744-4444 instead. Perhaps an advanced 911 service might cut back on the fake calls they're supposedly plagued with since such systems immediately trace back the number calling and do an instant CNA on it.

(Write to 2600, Box 752, Middle Island, NY 11953 or MCI Mail ID: 2600.)

August 1984

READER FEEDBACK

Dear *2600*:

Here's the latest info on phone scramblers.

Phone scramblers/descramblers are a type of device which allows one to communicate over the phone without anyone being able to hear your conversation in between the source and destination of the call. They are perfectly legal to own and operate, but there is one catch.

(The following information was obtained from a phreak who worked with an ex-CIA agent—to verify the validity of this statement.) The CIA, working in conjunction with AT&T, has the right to legally tap up to 600 phone lines in the U.S. The way that they are able to do this is that Bell Telephone can "test" your line any time it likes to see if it is working in proper order. Under the new ESS telephone system, finding scramblers/descramblers is very easy and once you are found, an instant file is generated on both the sender and the receiver of the call. They (CIA) will also do their best to try and crack your scrambler code. I have been told that they are extremely good at this. My advice to those of you out there thinking about building such a device is to seek other ways and for those of you currently using them to stop. Using these devices is simply waving a flag to AT&T and CIA saying, "I've got something important to say, and I don't want you to hear it."

Agent Orange

Dear Agent:

Thanks for the info and for the warning. While you're most probably correct about the powers that be taking a strong interest in any person using such a device, it seems absurd that we should have to constantly live in fear of having our privacy stripped, simply because we desire a little privacy!

We face some real problems in the near future if surveillance continues to grow and not enough is done by individuals to curb it. Technology is a deadly weapon *for anyone*..

Stay alive, awake, and indignant—you can't lose. Thanks for writing.

Dear *2600*:

I just had a horrible experience. As a faithful subscriber to this magazine, I keep all of my copies in a special loose-leaf book. This comes in very handy because they're not scattered all over the house, like most other things I possess. But last week, I dropped my loose-leaf book on the floor and of course it opened, scattering all of the pages here and there. Now, I have no trouble piecing together the first page of each issue, but I can't remember *where* the other ones belong, since they don't have any date on them! Can you help me piece them back together and take steps to ensure that this tragedy doesn't reoccur in the future? Thanks.

Miserable in Philadelphia

Dear MIP:

You've raised a very good point, one which we overlooked completely. While most of our stories are essentially "timeless", it does help to know when a certain article was printed. For this reason, we have begun (as of this issue) to number our pages in manual format. For instance, this is page 1-46 which means Volume 1, Page 46 of the year. We hope this eases the suffering. As far as previous issues, we will be coming out with a summary sheet towards the end of the year which we'll send to all subscribers. We'll try to get yours out early. And if anyone else knows of something we've overlooked or wants to make a suggestion, please write.

Dear *2600*:

I'm working on a book that gives the hackers' viewpoint and explains why he/she penetrates computer systems. I believe that even though I'm currently incarcerated, I could get a publisher to publish such a book.

To get this viewpoint I need help. I need the input of people who are active—the more the better. I also need the views of people who trash systems too. All I've ever seen is the viewpoint of the law enforcement agencies, media, business, and hackers that are caught etc. etc. etc. It's time your views were heard.

What I would do is just edit letters etc. sent to me and use these as basis for the book. By edit I mean pick the ones to be used in their entirety.

People interested in helping me with this can write to me under handles or pen names at the following address. *Do not use your real name or address as my mail is censored by officials here.*

John Gregg
Box 1000
Marion, IL 62959

A CORRECTION

In our last issue, we erroneously gave our MCI Mail ID as 2600. We didn't think there would be any problem in obtaining that ID, but there was. The MCI Mail computer apparently can't handle all-digit usernames. Our MCI Mail ID therefore, is 26HUNDRED. Write to us there or at our mailing address or our new telex address, all of which are listed on page one. (Especially write to us if you can think of any new places to have an address!)

September 1984

LETTERS FROM THE OUTSIDE

Dear *2600*:

Would you explain these terms to me? I don't know what they are:

1) phone loop
2) WATS extender.

Also, what became of *TAP*?

Thanks.

AZ

Dear AZ:

Phone loops are basically test circuits that the phone company uses for various purposes. They were never intended for use by the public. The way it works is simple. One caller dials number A. Another caller dials number B. When both of these people call these numbers at the same time, they become connected! Some loops make clicking or beeping sounds every few seconds which makes talking on them rather hard. But others are crystal clear connections. But while they may serve a purpose for the telco, what possible use could they be for anyone else. Well, for one thing, in many cases there is no charge for calling a loop number since they fall within a series of test numbers the phone company uses. Loops are also a great way to have an anonymous conversation—it's an indirect connection to another person instead of a direct one, although it's far from impossible to be traced while using one. Finally, there's the old call-collect trick where one person calls up one end of a loop that is within his local calling area. A friend from far away calls the other end of the loop collect. When the connection is made between the two loops, the operator will think that somebody answered the phone and will ask them if they want to accept a collect call. The telephone company winds up billing themselves for the call. Also, your phone number need never be known by the person "meeting" you on the loop, since he's not ever dialing your number. Loops have two ends—the silent end and the tone end. When a connection is established, the tone stops and conversation can begin. Loops are almost always found within the phone company test numbers (the 99XX suffix, in many cases). Loops are slowly but surely dying out, however.

An extender is very similar to a Sprint or MCI dialup, except that it's a number used exclusively by a particular business or organization for their phone calls. A WATS extender is one that is available on an 800 number. An employee calls up, hears the dial tone, enters a code, and dials away. There are many extenders around and many different types. Watch for an article soon detailing these.

As far as *TAP*, we sent a message to their MCI Mail account, and this is what their editor said:

"*TAP* is in hiatus. I was evicted from my apartment last week, put everything I could carry into storage, and left for California on vacation. When I get back to the East Coast, I'll be getting together issues 91 and 92. (While there is a possibility of getting the issues out while I'm out here, I will not put *TAP* out in California due to the restrictive state laws on proprietary information.)

MCI Mail is a viable way of asking me questions that require only short responses, but you should send me hard copy to *TAP*'s maildrop address (RM 603, 147 West 42nd St., New York, NY 10036) because I seldom check my MCI Mail anywhere near a hard copy printer. MCI usually deletes my mail before I can call back in and pull it out on paper.

Hope this answers your question. Keep Smiling, Chesire."

October 1984

LETTERS FROM THE OUTSIDE WORLD

Dear *2600*:

I am currently involved with the Crystal Palace BBS, formerly OSUNY (hopefully you have heard of it). The system is down now for some software modifications, and many people have tried to persuade me into changing the purpose of the board, which is telecommunications and other related fields. The crackdown on this type of BBS is starting to become overwhelming. This is what my inquiry is about. After reading my first copy of your newsletter, I was elated with the quality and content of information it had! Referring to the article "Look Out, He's Got a Computer!" I agree that the anti-computer hysteria has gone and is going to go too far! I am interested to know what exactly is an illegal BBS message and what is not. Do I have to monitor the system 24 hours a day, 7 days a week? Am I responsible for every message posted on the board? I know that these are questions that everyone wants answers to and can't find. As I see it the BBS is just another form of newsletter, so why are they picking on us?! I do, however, realize that some messages are quite illegal like: credit card #'s and the like, but the information on how to get those #'s is not illegal (right?). Any information on this subject would be greatly appreciated.

Crystal Palace

Dear CP:

What is a BBS? You know the answer, we do, and a good many of our readers also do. The problem is that the people who go around passing laws and raiding homes don't have the slightest idea what a BBS really is. All they care about is the fact that a computer is involved somewhere along the line. And computers, they say, can do anything in the world. But what's so ironic in the case of a BBS is the fact that the computer is just *storing messages!!* The exact same effect could be accomplished on a physical bulletin board, inside an auditorium, or in everyday conversation. But you don't see these things being outlawed because people would never stand for that kind of repression (we hope). Computers are easy targets because the average person doesn't understand them at all. By making people think that it's actually illegal to write something down and pass it along to others, the authorities are taking one great big step towards total control.

We agree that a BBS is really another form of newsletter. We don't agree that messages containing credit card #'s are illegal in any sense. (They are boring, though, and practically useless to anyone except fraud investigators.) It's the actual use of these numbers that constitutes fraud, not the simple act of passing them around. If a cop on the street overheard you giving numbers to a friend, could he arrest you? Let's hope it hasn't reached this stage.

We're currently working on getting some more legal information concerning this subject so that we can address your questions better. In the meantime, though, we hope your board and the many others like it around the world won't be intimidated by these scare tactics. You can talk about whatever the hell you want. But it's still illegal to commit the crimes you're talking about.

If enough of you guys stood up for your rights out in the open, this wouldn't be such a problem. You might actually wind up saving an important part of democracy for a few more years.

By the way, readers, if you're running a BBS that talks about these things or know of one that does, send in the name and phone number for our Hot 100 list which will be published soon. Make sure the BBS you're sending *wants* to be publicized and try to include a reason or two why your BBS is better than most. Check the front page for our addresses.

Dear *2600*:

Received your August issue, and enjoyed it. A number of comments...

1) Does anyone know what happened to *TAP*?

2) There is a newsletter called the *Comsec Letter*, available for free from Ross Engineering Assoc., 7906 Hope Valley Court, Adamstown, MD 21710. Lots of good information, but they want a letter requesting the newsletter on letterhead and identifying your interest in communications security (one can't be too careful these days!). It's always interesting to know what's happening on the other side...

3) What works against an ESS switch? Black boxes are ok, but more modern equipment seems to be coming in rapidly, blowing our older techniques off the air!

The Animal

Dear Animal:

For info on *TAP*, consult our September letters column. We hate repeating ourselves *all* the time.

Thanks for the sample copy of *Comsec Letter*. It looks interesting and we're looking into reprinting some of the good stuff. Readers: feel free to send us *anything* that looks like it might be interesting to us. It usually is.

ESS switches and black boxes are dealt with extensively in our August issue, as you probably know. The only thing we can suggest to counter an ESS is ingenuity. There's always a way to get around anything.

Dear *2600*:

I really enjoy your publication! It seems you guys are not a bunch of wimps who are so damn paranoid that the feds are going to catch you. Anyway, what types of back issues do you have? I received my first issue, which is Volume 1, Number 9. What are the context of the back issues? I'm looking for one having to do with loops, sprinting, hacking out sprint/mci's, or anything similar. Also, any arpanet/archnet stuff?

kd

Dear kd:

We'll be publishing a guide to our back issues that should be out right in time for the Christmas rush. Just about all of the topics you mentioned have already been covered and they all will be covered in the future. We accept articles and information from anyone.

You're quite correct in saying that we're not paranoid. We have nothing to be paranoid about because we're not doing anything wrong.

Dear *2600*:

Though it may seem like only yesterday that computer crime first caught the nation's fancy, it has been on the mind of state legislators for quite some time. With the recent passage of computer crime laws in Maryland, Iowa, Connecticut, and Hawaii, the number of states *lacking* computer crime laws has fallen to seventeen. The laws of the other 33 have been collected in a new reference work published by the National Center for Computer Crime Data, and called *The Computer Crime Law Reporter*. In the course of compiling the texts of all the state computer crime laws on the books, editor Jay BloomBecker found that a number of states had bills on the books for years without anyone noticing them.

The book, 200 pages plus two updates, is available for $45 from the National Center for Computer Crime Data, 4053 J.F.K. Library, California State University at Los Angeles, 5151 State University Drive, Los Angeles, CA 90032.

In addition, the National Center will begin publishing a newsletter devoted to morals and ethics in computing. Its name is *Conscience in Computing*.

There are schools teaching computer ethics, no matter how many are not. There are professionals questioning their roles as computer scientists and asking about the social impact of their work. There are computer bulletin boards which support ethics discussion groups.

Conscience in Computing will be a monthly newsletter, subscriptions costing $18 annually. Work exchanges allow readers to become subscribers by convincing others to subscribe, reporting news of conscience in computing, or working out an individual contract with the National Center. Interested people can write to the above address.

The National Center for Computer Crime Data

(The National Center for Computer Crime Data is a nonprofit research organization at California State University at Los Angeles.)

Whoopsee

In our last issue, we forgot to mention that in our August issue, we forgot to mention that the front page story ("But How Does It Work?") came from the desk of BIOC Agent 003. Better late than never.

November 1984

Letters From All Over

Dear *2600*:

I've been a subscriber to *2600* for some time now, and I enjoy the publication. You're doing a nice public service by illuminating the often neglected area of telephone technology and operations.

One way in which *2600* could do an even more interesting job is by printing a bibliography or list of references from time to time. What books, articles, and journals provide additional information about the telephone system? For example, one article covered ESS #5; there must be some articles, advertisements in trade publications, etc., that provide additional information.

I can give you a start which hopefully you and other readers can add to. Here are two books:

Notes on Long Distance Dialing, published by AT&T around 1971.

Telephone Accessories You Can Build, by J. Gilder, around 1975.

Many thanks. Keep up the fascinating work!!

Sincerely,
Howard A. Karten
Randolph, MA

Dear Mr. Karten:

You'll be happy to know that we've broken ground on a database for phreaker/hacker required reading. Your two suggestions are the first entries. A couple of others that we were able to come up with off the tops of our heads:

The Phone Book by J. Edgar Hyde.

Notes on the Network by AT&T themselves. This one is reportedly *out of print* altogether!

Add to that *The Rise of the Computer State* by David Burnham, which we reviewed here a few months back and *The Puzzle Palace*, a fascinating work on the NSA.

We'll do our best to expand on this list, but we really need the help of our subscribers on this one. If you know of a good book or publication, send the name of it to us, or call us and tell us about it. An easy way to find material is to go to your local library and look in the card catalog under the subject: Telephone or Computer. There's bound to be something interesting nearly everywhere and if a lot of people do this, we'll have quite a list before we know it! (By the way, if you hit a card catalog, be sure to drop in your own card with our address on it so that our fame can continue to spread cheaply.)

Dear *2600*:

I have been silver boxing on various directory assistances and have found that pressing a one starts a ringing. Is this just a test function or is it going somewhere?

Thanks,
Fire Monger
Arlington, VA

Dear Fire:

For the benefit of others, we'll briefly explain a silver box. Every touch tone® phone actually has the capacity for sixteen tones, not just twelve. A simple modification inside the phone accomplishes this. The extra tones (a vertical row to the right of the 3-6-9-# row) are labeled A-B-C-D. These tones are used primarily on Autovon, or Pa-Bell, the military phone network which can knock out civilian phone service at any time for its own purposes. (Look at the phones on the walls in *War Games*.) Such a modified phone is labeled a "silver box". But the tones don't really do all that much good to people outside the military, unless they've *somehow* tapped into a military phone system. This, however, is impossible. Isn't it?

What most phreaks use silver boxes for are zapping long distance info. You would call XXX-555-1212 and then hold down the D key. The moment the information operator picks up, the D tone cuts her off and gives the caller a pulsing dial tone. Each number you hit at this point has a different effect. In some areas, hitting a 6 connects you to one end of a loop. (7 is the other end.) Another number gives you a carrier! We haven't heard of anybody who could do anything with it, though. And hitting a one usually gets a ringing somewhere. It almost always sounds exactly like the directory assistance ring for that area. We have never heard of anyone picking up on such a ring, so logic tells us that it's simply a test. If anyone knows otherwise, please let us know.

Incidentally, since it now costs 50¢ to call long distance information, silver boxing has experienced a slight lull.

Dear *2600*:

In reply to *Getting Caught: Hacker's View* — I was in the reverse situation. I had turned in a close friend last spring. I was faced with a situation of turning him in or being an accomplice to fraud. Being in a spot like that, no one can make a decision to do *that* without always doubting yourself, choosing between being an accomplice or keeping a friendship is a place I wouldn't wish for my worst enemy. In dealing with the feds, one can't take everything as truth — they tell the guy who's busted one story (in hopes of making him crack) and tell the "informer" another story (in hopes of scaring them into saying things they wouldn't normally say). The people who read that in *2600* probably thought the person who turned this guy in was a rat, a fink, or a fed. What they may not realize is the other side of the story, the part where the 'informer' gets cornered into telling what he knows, or sacrifice his freedom (end up in jail) if he doesn't tell. In my case, that's what happened. I was cornered and had to tell and provide evidence in order to keep my ass clean. The guy I turned in had fouled up the job and would've been caught without my telling, though him and his friends still think I'm a rat. What they may not realize is what they would've done if they were me. Would they have gone to jail to protect a friendship? Or would the friend you're protecting do the same for you if he were faced with turning you in or going to jail? The other point being that since he would've been caught anyway, I would've been subpoenaed to testify against him because he had involved me by using my property for the fraud. To tell a friend you're going to commit some fraud (or whatever) is not a crime, but using that person's property and by that, making them an accomplice, is.

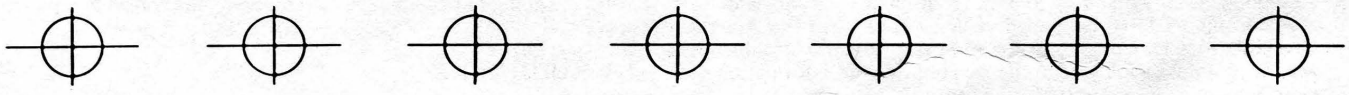
Signed,
The Trojan Horse

Dear Trojan:

Thanks for writing and giving us an even more ignored side of the story. You may have opened up some eyes. Try letting your "friend" see this letter and he might realize that he wasn't the only one going through hell on a rubber raft.

Last month, we told you about the COMSEC Letter. It is no longer free. It now costs $25. It is free, though, to members of the Communications Security Association (CSA). This is a new group for people interested in communications security. They will soon have a BBS, in addition to publications, seminars, and workshops. The dues are $50 per year. For more info, write to CSA, 655 15th St., Suite 320, Washington, DC 20005 or call 2026394620.

We also found out about another magazine—Boot-Legger. It costs $25 a year and their address is 3310 Holland Loop Road, Cave Junction, OR 97523.



For all those individuals who are willing to write or participate in the production of 2600, the following is a partial list of the types of things we would like to see, be they articles or clippings or raw data or something else. Remember, we are a community newsletter—the community being those who chance or choose to read or participate in 2600.

(articles can be in just about any format and any length. the only thing we ask is that they be reasonably legible.)

fact	**fiction**	**transcripts**	**lists of #'s**	**computer dial-ups**	**bulletin boards**
technical stuff	**phone alterations**	**decoders**	**book reviews**	**software reviews**	**bbs reviews**
sundries	**govt documents**	**inside telco stuff**	**garbage**	**phone books**	**pictures**
news articles	**legislation**	**security companies**	**opinions**	**essays**	**japan's telco**
any foreign telco	**alternate telcos**	**big brother stuff**	**experiences**	**telco employees**	**viral programs**
malicious hacking	**malicious phreaking**	**social engineering**	**roots of telephony**	**switching systems**	**dictionary of terms**
divestitures	**telco policy**	**dial-it #'s**	**literature**	**political use of comp.**	**dissident use of comp.**
infomania	**ibm & south africa**	**credit card info**	**bank machines**	**cable tv**	**strange phones**

please do whatever you can so that 2600 will always be interesting. write to us or call us at the numbers on the front cover.
IF YOU HAVEN'T SENT IN LAST MONTH'S BLUE SURVEY CARDS, DO IT NOW!!!!!!! THANKS.

December 1984

We've tallied up all of the blue cards that were returned and the latest results are to the right. Below are selected subscriber comments with occasional retorts by us.

AS OF 12/10/84 AT 23:47:53 THE BLUE CARD SURVEY RESPONSES WERE: 58% OF THE CARDS WERE RETURNED. OF THESE 94.8% SAID THEY WOULD RENEW. AN AVERAGE OF 3.24 PEOPLE PER SUBSCRIBER READ 2600. 77.6% OF THE RESPONDENTS USE OUR LOOSE-LEAF HOLES. 81% SAID THEY WERE SATISFIED WITH 2600. REASONS FOR READING: 58.6% PERSONAL, 55.2% HOBBY, 19% BUSINESS, 1.5% SECURITY AGENCY, 1.7% INDUSTRY, 20.7% OTHER. 15.5% SAID WE WERE TOO TECHNICAL AND 22.4% SAID WE WERE NOT TECHNICAL ENOUGH. 55% SAID WE WERE JUST RIGHT. FINALLY, 62.1% PROMISED TO CONTRIBUTE ARTICLES IN THE FUTURE.

AUSTIN, TEXAS—"The info is generally more useful (and less anti-social) than TAP...it's entertaining. What format should I use on articles?"

ARTICLES CAN BE OF ANY FORMAT. JUST TRY TO MAKE IT LEGIBLE. THEY END UP GETTING RETYPED NO MATTER WHAT. YOU CAN ALSO CALL IN STORIES USING THE PHONE NUMBER ON THE FRONT PAGE.

ALASKA—"One of the best sources for detailed information on telecommunications. Also a good source for phreak information. I wish you would put the back page of each issue to better use though! ...For me, it borders on too technical, but I don't mind because I'll learn more that way."

MARINA DEL REY, CALIFORNIA—"I like *2600* because of the stories on hackers etc. getting caught. Also because of the tips!"

TUCSON, ARIZONA—"Have trouble understanding the jargon. Facts sometimes printed without explanations. Still don't know what '2600' means."

2600 HERTZ IS SIMPLY THE FREQUENCY USED BY PHONE PHREAKS TO SEIZE CONTROL OF A PHONE LINE. OH YES, THE PHONE COMPANY USES IT TOO; YOU MAY HEAR A COUPLE OF 2600 HERTZ TONES (TWEEPS) AT THE END OF A PHONE CALL.

VIRGINIA—"Too much was already printed in BIOC's tutorials or is too general."

ANCHORAGE, ALASKA—"It's awesum, could do with sum box plans. Send information on Alaska's telefone system."

OK, FIRST PERSON TO SEND US WORKING BLUE BOX PLANS GETS 10 FREE ISSUES.

ALBANY, NEW YORK—"Poor choice of filler for last page this month [October]."

LOS ANGELES, CALIFORNIA—"You need more business watching—somebody has to keep an eye on the Harvard Business School, IBM, ATT crowd. Information has become big business, guys! Hackers are the new Judas goats. We dreamed that micros would make freedom of information real. Meanwhile, American Business bought 90% of the *world's* commercial databases. Hackers and free bulletin boards are anathema to those who think of information as a commodity to be brokered and controlled. And for "technical" reasons, the phone companies wish you to register your modem. Sound paranoid? Investigate the relationship between Big Blue and South Africa."

SAN JOSE, CALIFORNIA—"Good stuff—where else would I get it? Keep it up!"

FT. LAUDERDALE, FLORIDA—"I am very satisfied with the content. In fact, if you could put more in that would be great. I can't get enough of *2600*."

NEW YORK, NY—"You do not get enough original material. August's issue was plagerized from Basic Telcom V."

LOOK UP THE DEFINITION OF PLAGIARIZE. THE ARTICLE YOU'RE REFERRING TO WAS GIVEN TO US BY THE AUTHOR HIMSELF.

NEW YORK, NY—"Sometimes too technical..."

BRYAN, TEXAS—"It's really good. Need more information how-to's on neat things with phones."

NEW JERSEY—"It is a well rounded publication. More telecommunication's hobbiest articles. For your Hot 100 BBS's add the Armour at 2012671207. 10 Meg online and a friendly sysop. No charge for validation and over 280 general interest files."

BOSTON, MASS.—"The back page usually sucks (repro from telephone book or something)."

JAMAICA, NY—" 'Hacker's View', a *great* article!"

WEST VIRGINIA—"Like the articles. Info is good but I have no idea what a lot of abbreviations stand for or what makes switch equipment work..."

SAN FRANCISCO, CALIFORNIA—"It seems to fill a gap left by TAP. I also find your 'Newsflash' section especially useful in bringing several sources of info together."

WESTCHESTER, NY—"*2600* is the one newsletter where 'you get your money's worth'. *2600* provides information for those who wish to learn. A friend and myself love to tamper physically with phones and have come up with some nice plans for 'additions' which are legal and practical."

TELL US WHAT AND TELL US HOW!

WISCONSIN—"I find it very informative, although I wish it would go deeper into the technical aspects of the network."

SALT LAKE CITY, UTAH—"Could use less of the telco graphics and have more info useful to hackers, infomaniacs, etc. Keep publishing!"

SUFFERN, NEW YORK—"Informative...could be a little more technical."

NO POSTMARK (!)—"Good stuff. Try connecting your magazine with other sources: boards, AE lines, TAP, etc."

WE'RE OPEN TO SPECIFIC SUGGESTIONS.

TRENTON, NJ—"I think it should be more like TAP with underground information."

LOUISVILLE, KENTUCKY—"More news. More about bulletin boards. Fewer ads from old phone books...I sent $10 to TAP at the same time I subscribed to *2600*. But TAP neither honored the subscription nor cashed the check. Can you help?"

LOOK AT IT THIS WAY. IF NEWSWEEK RIPPED YOU OFF, WOULD WE BE ABLE TO DO ANYTHING? SAME THING HERE.

DENVER, COLORADO—"Some of it blows me away but some of it is just right. This reader response was a good idea. Keep it up."

MIDDLESEX, MASS.—"I think oftentimes your last page sucks. Aside from that I think you are cool. More stuff is needed about individual systems though."

SALINAS, CALIFORNIA—"Please have more technical explanations of phone and/or computer systems, or refer to more sources of info."

TRENTON, NJ—"Too technical—looking for the old zap of TAP."

SPEAKING OF WHICH, WHERE THE HELL IS THAT OLD ZAP?!?

DENVER, COLORADO—"Needs more codes."

IT'S ALWAYS BEEN OUR POLICY NOT TO PROVIDE CODES SO MUCH AS PURE KNOWLEDGE.

PHILADELPHIA, PA—"The phone articles are great. However, I get lost in the computer stuff. I enjoy reading stories (fact *or* fiction) with an adventurous flair."

MIAMI, FLORIDA—"I think a little longer with more topics would improve it. Also, start each article in layman's terms."

WORCESTER, MASS.—"The articles are good, but useful info would be better than articles."

SUCH AS?

TORONTO, CANADA—"I'd like more commentary and criticism on the general policies of telco's and more tutorial material on the technology. Too technical, but don't drop the technicalities—just *explain* them."

BROOKLYN, NY—"Excellent and outrageous."

PITTSBURGH, PA.—"I have quit the hobby of phreaking, although I am still interested in it. The *time* involved, money saved, and mainly *the excitement of it* is not worth the risk, stress, and ruining my life (who knows?). I am a junior engineering student and want to stay that way and keep my friends. I regret that I can not continue phreaking, hacking. I will miss it!"

IT'S DOUBTFUL THAT RENEWING YOUR SUBSCRIPTION WILL RUIN YOUR LIFE. IF YOU'RE STILL INTERESTED, AS YOU SAY, THEN WHY NOT READ ABOUT IT AND TALK ABOUT IT? THEY HAVEN'T OUTLAWED THAT YET. IT'S CLEAR THAT YOU'VE BEEN INTIMIDATED AS WE ALL HAVE TO A DEGREE. GOOD LUCK EITHER WAY.

Thanks for returning the cards, folks. We'll try to follow your suggestions and do something about the back page. Thanks also to those of you who made financial contributions, which we can always use. Hopefully, next year such contributions will be tax-deductible.

Did you know that you can get two free months of 2600 if you get a friend or loved one to subscribe? You probably didn't know that, since this is the first time we ever mentioned it. But it's true. Just have the new subscriber mention your name and we'll add two months to your subscription.

In addition to the index which we're enclosing with this issue, there is also a 2600 1984 Table of Contents, a page by page guide to all of the issues. It costs $1 and should be placed at the very beginning of your collection.

Page 5

The idea behind “Page 5” was to simply print data of one sort or another, often without explanation, on a regular basis. In 1984, data was precious and many of us lived for information. Sometimes we were real wise guys about it, printing a supposedly sensitive White House phone list as a tutorial on how to properly use tabs. Other times, we printed things that today wouldn’t seem like a big deal (a list of all of the country codes in the world or dial-up numbers to various corporate services), but we were information-hungry back then and there weren’t a whole lot of places to go to get this sort of thing. A list of networks on the Defense Data Network was something most people hadn’t a clue about, but it sure sounded interesting. We also took a bit of flack for printing a bunch of old ads from telephone books on a couple of occasions. Looking back, we think they’ve aged rather well.

“Page 5” usually continued onto the sixth and last page, but there were occasions when some other graphic or article would appear there instead. The feature appeared in every 1984 issue except July, when we ran a special article on TRW access. However, the “Page 5” title was left in and the article was presented as if it were data in the original run. We don’t know what we were thinking.

Position	Name	Extension
Office of the President		
The President	Ronald Reagan	2858
Special assistant	David C. Fischer	2168
Personal secretary to the President	Kathleen Osborne	2858
Office of the Counselor to the President		
Counselor to the President	Edwin Meese III	2235
Deputy counselor	James E. Jenkins	7600
Assistant counselor	Edwin W. Thomas Jr.	2235
Special assistant	Mitchell F. Stanley	2235
Assistant to the President for Cabinet affairs	Craig L. Fuller	2823
Secretary	Adela Gonzalez-Nardi	2823
Assistant director	T. Kenneth Gribb Jr.	2800
Administrative assistants	Karen Hart	2823
	Nancy A. (Missy) Hodapp	2800
Director of planning and evaluation	Richard S. Beal	6690
Office of Chief of Staff		
Chief of staff	James A. Baker III	6797
Executive assistant to the chief of staff	Margaret D. Tutwiler	6797
Staff assistant	Kathy Camalier	6797
Confidential secretary	Margaret Glasscock	6797
Deputy to the chief of staff	Richard G. Darman	2702
Administrative assistant	Sara Currence Emery	2702
Secretary	Janet F. McMinn	2702
Special assistant to the chief of staff	James W. Cicconi	2174
Presidential correspondence	Anne Higgins	7610
Special presidential messages	Dodie Livingston	2941
Office of the Deputy Chief of Staff		
Deputy chief of staff	Michael K. Deaver	6475
Assistant to the deputy chief of staff	Joseph W. Canzeri	2861
Staff assistant	Shirley Moore	6475
Special assistant to the President for private initiatives	James S. Rosebush	2957
Executive assistant	Bernyce Fletcher	2957
Director of special support services	Edward V. Hickey Jr.	2150
Deputy director of special support services	Dennis E. LeBlanc	2150
Deputy director of military office	Col. Frank E. Millner	2150
Army aide to the President	Lt. Col. Jose A. Muratti Jr.	2150
Air Force aide to the President	Maj. William M. Drennan	2150
Navy aide to the President	Cdr. William R. Schmidt	2150
Marine Corps aide to the President	Maj. John P. Kline Jr.	2150
Physician to the President	Dr. Daniel Ruge	2672
Director of advance	Stephen M. Studdert	7565
Deputy director of advance	Hugh L. O'Neill	7565
Administrative assistant	CeCe B. Kremer	7565
Trip desk officers	Marti J. Frucci	7565
	Karen Jones Roberts	7565
	Lynn Smallpage	7565
Advance staff	Robert K. Gubitosi	7565
	James F. Kuhn	7565
	Dan Morris	7565
	Lanny F. Wiles	7565
	Rocky D. Kuonen	7565
Director of scheduling	Gregory Newell	7560
Deputy director of scheduling	Tricia Rodgers	7560
Administrative assistant	Cristy Valentine	7560
Staff assistants	Michael Castine	7560
	Frances (Fan) Snodgrass	7560
	Netta A. Dickey	7560
Confidential assistant	Mary H. Rawlins	7560
President's diarist	Ellen Jones	7560
Appointments secretary	Helen C. Donaldson	7560
Staff directory for the First Lady	Peter McCoy	6702
Administrative assistant	Christine J. Hathaway	6702
Press secretary	Sheila P. Tate	7136
Assistant press secretary	Barbara Cook	7136
Personal secretary	Elaine Crispen	6633
Social secretary	Muffie Brandon	7064
Assistant social secretary	Linda Faulkner	7064
Scheduling director	Nina Wormser	7910
Special projects	Ann Wrobleski	7905
Office of the Vice President		
The Vice President	George Bush	7123
Executive assistant	Charles G. (Chase) Untermeyer	2587
Chief of staff	Daniel J. Murphy	6606
Deputy chief of staff	Richard N. Bond	7056
Military assistants	Lt. Col. Michael D. Fry	4213*
	Lt. Col. William Eckert	4223*
Counsel	C. Boyden Gray	7034
Deputy counsel	Rafael V. Capo	7034
Press secretary	Peter Teeley	6772
Deputy press secretary	Shirley M. Green	6772
Speechwriter	Christopher Buckley	7453
Domestic policy adviser	Thaddeus A. Garrett Jr.	2173
Assistant domestic policy adviser	Mary S. Gall	7935
National security affairs adviser	Nancy Bearg Dyke	4213
Congressional relations assistant	Robert V. Thompson	224-2424
Legislative assistant	Susan Alvarado	224-8391
Assistant for appointments and scheduling	Jennifer Fitzgerald	7870

All telephone numbers are on the 456- exchange except those marked with an asterisk, which are on the 395- exchange, and those listed in full.

Proper tabbing is extremely important when typing a list. Above is an example of tabs used successfully.

AFGHANISTAN - 93
ALBANIA - 355
ALGERIA - 21 - 3, 4, OR 5 *
ANDORRA - 33 - AP 078
ANGOLA - 244
ARGENTINA - 54 - 1, 21, 41, OR 51
AUSTRALIA - 61 - D1-3
AUSTRIA - 43 - D4
BAHRAIN - 973
BANGLADESH - 880
BELGIUM - 32 - D1-2
BELIZE - 501
BENIN - 229
BHUTAN - * - 1400 PHONES
BOLIVIA - 591
BOTSWANA - 267
BRAZIL - 55 - D2 (X1)
BRUNEI - 673
BULGARIA - 359
BURMA - 95
BURUNDI - 257
CAMEROON - 237
CAPE VERDE - 238
CENT. AFRICAN REPUBLIC - 236
CHAD - 235
CHILE - 56 - D1-2
CHINA (MAINLAND) - *
COLOMBIA - 57 - D3 OR D5
COMORO IS. - 269
CONGO - 242
COSTA RICA - 506
CUBA - *
CYPRUS - 357 - D2 (X1)
CZECHOSLOVAKIA - 42
DENMARK - 45 - CODES 1-9, FAROES IS 42
DJIBOUTI - 253
DOMINICA - *
ECUADOR - 593 - D2 OR D4
EGYPT - 20
EL SALVADOR - 503 - D2 OR D4
EQU. GUINEA - 240
ETHIOPIA - 251
FALKLAND IS. - *
FIJI - 679
FINLAND - 358 - CODE 0 OR D2
FRANCE - 33 - CODE 1 OR D2
FRENCH GUIANA - 594
FR. POLYNESIA - 689
GABON - 241
GAMBIA - 220
GERMAN DEM. REPUBLIC - 37 - D1-5
FEDERAL REP. OF GERMANY - 49 - D2-4
GHANA - 233
GIBRALTAR - 350
GILBERT IS. - 686
GREECE - 30 - CODE 1 OR D2-3
GRENADA - *
MACAO - 853
MADAGASCAR - 261
MALAWI - 265
MALAYSIA - 60 - CODES 3 OR 5
MALDIVES - *
MALI - 223
MALTA - 356
MARIANA IS. - *
MARTINIQUE - 596
MAURITANIA - 222
MAURITIUS - 230
MEXICO - 52
MONACO - 33
MONGOLIA - 976
MOROCCO - 21 - CODES 0, 1, OR 2 *
MOZAMBIQUE - 258
NAURU - 674
NEPAL - 977
NETHERLANDS - 31 - D2 OR D4
NETH. ANTILLES - 599 - D1
NEW CALEDONIA - 687
NEW HEBRIDES - 678
NEW ZEALAND - 64 - D2-5
NICARAGUA - 505 - D1-2
NIGER - 227
NIGERIA - 234 - D2-3 (OXX)
NORWAY - 47 - D1-2
OMAN - 968
PAKISTAN - 92
PANAMA - 507
PAPUA NEW GUINEA - 675
PARAGUAY - 595
PERU - 51 - D2-4
PHILIPPINES - 63 - D1-4
POLAND - 48
PORTUGAL - 351 - D2
QATAR - 974
REUNION - 262
ROMANIA - 40
RWANDA - 250
ST. HELENA - *
AMER. SAMOA - 684
SAN MARINO - 39 - AP 541
SAO TOME (PRINCIPE) - 239
SAUDI ARABIA - 966 - D1-2
SENEGAL - 221
SEYCHELLES - 248
SIERRA LEONE -232
SINGAPORE - 65
SOLOMON IS. - 677
SOMALIA - 252
SOUTH AFRICA - 27 - D2 (X1)
S. W. AFRICA - 264
SPAIN - 34 - D1-2
SRI LANKA - 94
SUDAN - 249
SURINAME - 597

GUADELOUPE - 590
GUAM - 671
GUATEMALA - 502 - CODES 2 OR 61
GUINEA - 224
GUINEA-BISSAU - 245
GUYANA - 592
HAITI - 509
HONDURAS - 504
HONG KONG - 852 - CODES 3, 5, OR 12
HUNGARY - 36 - D1-2
ICELAND - 354
INDIA - 91 - CODES 11 OR 22
INDONESIA - 62
IRAN - 98 - D2-4 (XXX1)
IRAQ - 964 - D1-2
IRELAND - 353 - D1-2
ISRAEL - 972 - D1-2
ITALY - 39 - D2-3
IVORY COAST - 225

JAPAN - 81 - D1-2
JORDAN - 962
KAMPUCHEA - 855
KENYA - 254 - AP 2
N KOREA - *
S KOREA -82 - D2
KUWAIT - 965
LAOS - 856
LEBANON - 961
LESOTHO - 266
LIBERIA - 231
LIBYA - 21 - CODES 8 OR 9 *
LIECHTENSTEIN - 41 - AP 75
LUXEMBOURG - 352

SWAZILAND - 268
SWEDEN - 46 - D1-3
SWITZERLAND - 41 - CODE 1 OR D2
SYRIA - 963
TAIWAN - 86 - D1-2
TANZANIA - 255
THAILAND - 66 - AP 2
TIMOR - 672
TOGO - 228
TONGA - *
TRINIDAD - *
TUNIS - 21 - CODE 2 OR 6 *
TURKEY - 90 - D2 (X1)
TURKS & CAICOS - *
TUVALU - *
UGANDA - 256
UAE - 971/978/979
UK - 44 - D1-3 - 25 MILLION PHONES
USA/CANADA/CARIBBEAN - 1 - D3 (XOX OR X1X)
- 190 MILLION PHONES
UPPER VOLTA - 226
URUGUAY - 598
USSR - 7 - 20 MILLION PHONES
VATICAN CITY - 39 - AP 6
VENEZUELA - 58 - D1-2
VIETNAM - 84
WEST. SOMOA - *
YEMEN - 967
YEMEN PDR - 969
YUGOSLAVIA - 38 - D2 (X1)
ZAIRE - 243
ZAMBIA - 260
ZIMBABWE - 263

DEFINITIONS:

DX - X REPRESENTS THE NUMBER OF DIGITS IN A COUNTRY'S CITY CODES. CAN BE OF A RANGE 'DX-Y' BETWEEN X AND Y DIGITS.

(X1) TYPICAL ROUTING CODE. X CAN BE ANY DIGIT. 1 IS ARBITRARY.

AP - ALL POINTS. USE THIS IN FRONT OF ANY LOCAL NUMBER.

CODE REPRESENTS AN INDIVIDUAL CITY CODE. USE ANY OF THE CODES LISTED, OR IF ANOTHER RANGE IS SPECIFIED, ALSO FOLLOW THAT FORMAT.

* USE INTERNATIONAL OPERATOR EITHER FOR ALL CALLS TO THAT COUNTRY IF NO CODE IS LISTED, OR FOR CALLS TO PARTICULAR AREAS DENOTED BY THE '*'.

NOTE: USA COUNTRY CODE '1' COVERS ALL OF THE CONTINENTAL USA, ALL OF CANADA, ALASKA AND HAWAII, AND PORTIONS OF NORTHERN MEXICO. IN ADDITION, THE USA AREA CODE 809 COVERS PUERTO RICO, THE US AND BRITISH VIRGIN ISLANDS, AND VARIOUS OTHER CARIBBEAN ISLANDS. THE 709 AREA CODE IS ROUTED THRU CANADA TO COVER FRENCH POSSESSIONS IN THE HEMISPHERE, NOTABLY THE ISLANDS OF ST. PIERRE AND MIQUELON.

The following is a list of hosts that are accessible through ARPANet. ARPANet connects many systems together, allowing them to send electronic mail, transfer files, and be able to work on each other's computers. The network is very intricate, containing many subnets, including the one below, called "MILNET", short for "Military Network". That is, our military. This is a small list, encompassing approximately one twentieth the entire number of systems accessible through ARPANet. Notice the PENTAGON-TAC below. This is an access point for people in the government.

Host address:	Host name:	Host type:	Operating system:
26.0.0.3	NOSC-CC	VAX-11/750	UNIX
26.2.0.3	LOGICON	PDP-11/70	UNIX
26.3.0.3	NPRDC	VAX-11/780	UNIX
26.0.0.8	NRL	VAX-11/750	UNIX
26.1.0.8	NRL-AIC	VAX-11/780	UNIX
26.2.0.8	NSWC-WO	VAX-11/750	UNIX
26.3.0.8	NRL-TOPS10	DEC-10	TOPS10
26.6.0.8	NRL-ARCTAN	PDP-11/40	RSX11
26.7.0.8	NRL-CSS	VAX-11/780	UNIX
26.1.0.13	GUNTER-ADAM	DEC-2060	TOPS20
26.3.0.13	ATC-KEES1	BURROUGHS-B/29	BTOX/UNIX
26.0.0.14	CMU-CS-B	DEC-1050	TOPS10
26.6.0.16	RIACS-ICARUS	VAX-11/730	UNIX
26.0.0.17	MITRE	C/70	UNIX
26.0.0.18	RADC-MULTICS	HONEYWELL-DPS-8/70M	MULTICS
26.3.0.18	RADC-TOPS20	DEC-2040T	TOPS20
26.5.0.18	RADC-UNIX	PDP-11/45	UNIX
26.6.0.18	GE-CRD	VAX-11/780	VMS
26.0.0.19	NBS-VMS	VAX-11/780	VMS
26.1.0.19	NBS-SDC	VAX-11/780	VMS
26.2.0.19	NBS-UNIX	VAX-11/750	UNIX
26.3.0.19	NBS-PL	PDP-11/70	UNIX
26.6.0.19	NBS-AMRF	VAX-11/780	VMS
26.7.0.19	NBS-SSI	VAX-11/750	UNIX
26.4.0.20	DCA-EMS	C/70	UNIX
26.0.0.23	USC-ECLB	DEC-1090B	TOPS20
26.3.0.23	USC-ECL	DEC-1090B	TOPS20
26.0.0.24	NADC	VAX-11/780	UNIX
26.1.0.25	DDN1	C/70	UNIX
26.0.0.26	PENTAGON-TAC	C/30	TAC
26.3.0.26	TCACCIS-CSC	VAX-11/750	VMS
26.0.0.29	BRL	PDP-11/70	UNIX
26.1.0.29	APG-1	C/70	UNIX
26.3.0.30	ATC-RAND1	BURROUGHS-B/29	BTOS/UNIX
26.0.0.33	NPS	PLURIBUS	PLI
26.3.0.33	FNOC-SECURE	PLURIBUS	PLI
26.0.0.35	NOSC-SECURE2	PLURIBUS	PLI
26.1.0.35	NOSC-TECR	VAX-11/780	VMS/EUNICE
26.3.0.35	NOSC-SECURE3	PLURIBUS	PLI
26.4.0.35	NOSC-F4	FOONLY-F4	FOONEX
26.0.0.36	COINS-TAS	PLURIBUS	PLI
26.1.0.36	HAWAII-EMH	C/70	UNIX
26.0.0.39	EDWARDS-VAX	VAX-11/782	VMS
26.1.0.39	EDWARDS-2060	DEC-2060T	TOPS20
26.1.0.45	ARDC	VAX-11/780	UNIX
26.3.0.46	OKC-UNIX	PDP-11/70	UNIX
26.1.0.48	AFWL	PDP-11/50	RSX11M
26.0.0.49	BBNB	DEC-10	TENEX

26.0.0.50	DARCOM-TEST	VAX-11/750	UNIX
26.3.0.50	LSSA-DB1	NAS3-5	MVS
26.7.0.50	ETL-AI	VAX-11/780	VMS
26.0.0.53	AFSC-AD	PDP-11/45	RSX11M
26.2.0.53	AFSC-DEV	PDP-11/44	RSX11M
26.4.0.53	NCSC	VAX-11/750	UNIX
26.5.0.53	MARTIN	PDP-11/45	RSX
26.6.0.53	EGLIN-VAX	VAX-11/780	VMS
26.2.0.54	ACC	PDP-11/70	UNIX
26.1.0.55	ANL-MCS	VAX-11/780	UNIX
26.2.0.55	COMPION-VMS	VAX-11/750	VMS
26.0.0.57	TYCHO	PDP-11/70	UNIX
26.2.0.57	MARYLAND	VAX-11/780	UNIX
26.0.0.58	NYU	VAX-11/780	UNIX
26.1.0.58	BNL	PDP-11/44	UNIX
26.3.0.60	CECOM-1	FOONLY-F4	TENEX
26.0.0.61	STL-HOST1	DEC-2040	TOPS20
26.1.0.61	ALMSA-1	VAX-11/750	UNIX
26.1.0.64	MARTIN-B	VAX-11/750	VMS
26.3.0.64	ROBINS-UNIX	PDP-11/45	UNIX
26.0.0.65	AFSC-SD	DEC-2020T	TOPS20
26.2.0.65	AEROSPACE	VAX-11/780	UNIX
26.3.0.65	MARTIN-ED	PDP-11/45	RSX11M
26.1.0.66	AFGL	PDP-11/50	RSX11M
26.3.0.66	MITRE-BEDFORD	VAX-11/780	UNIX
26.0.0.67	AFSC-HQ	DEC-2040T	TOPS20
26.1.0.73	SRI-WARF	PLURIBUS	PLI
26.4.0.73	SRI-F4	FOONLY-F4	TENEX
26.0.0.74	SIMTEL20	DEC-2040T	TOPS20
26.1.0.74	WSMR70A	C/70	UNIX
26.3.0.74	WSMR70B	C/70	UNIX
26.3.0.78	MCCLELLAN	PDP-11/70	UNIX
26.0.0.81	NEMS	VAX-11/750	UNIX
26.1.0.81	NALCON	VAX-11/750	UNIX
26.3.0.81	DTRC	VAX-11/780	UNIX
26.0.0.82	BBNCCT	C/70	UNIX
26.3.0.82	DDN2	C/70	UNIX
26.4.0.82	BBN-RSM	PLURIBUS	PLI
26.9.0.82	TEP1	C/30	
26.0.0.87	SANDIA	DEC-2060T	TOPS20
26.0.0.88	NLM-MCS	VAX-11/780	UNIX
26.0.0.90	LANL	VAX-11/750	UNIX
26.4.0.92	NAVDAF-NEWPORT	UNIVAC-1100	CMS
26.1.0.95	S1-A	FOONLY-F2	WAITS
26.2.0.95	S1-B	VAX-11/750	UNIX
26.3.0.95	S1-C	VAX-11/750	UNIX
26.2.0.97	PAXRV-NES	VAX-11/730	VMS
26.1.0.103	USC-ISIE	DEC-1090T	TOPS20
26.2.0.103	ADA-VAX	VAX-11/780	VMS
26.3.0.103	USC-ISI	DEC-1090T	TOPS20
26.1.0.104	DCEC-LSUS2	IBM-158	MVS/SP
26.4.0.104	DCEC-LSUS	IBM-158	MVS/SP
26.3.0.106	ARPA-PNG11	PDP-11/34	EPOS
26.0.0.112	STL-HOST2	BBN-C/60	UNIX
26.0.0.117	KOREA-EMH	C/70	UNIX

MCI ACCESS NUMBERS

(Courtesy of Plovernet—5169352481)

AARON, OHIO	(216) 253-1490
ATLANTA, GA.	(404) 523-0003
AUSTIN, TEXAS	(512) 473-2716
BALTIMORE, MD.	(301) 321-8933
BOSTON, MASS.	(617) 482-2888
CHICAGO, ILL.	(312) 321-6581
CINCINNATI, OHIO	(513) 241-1216
CLEVELAND, OHIO	(216) 621-2371
COLUMBUS, OHIO	(614) 224-0970
DALLAS, TEXAS	(214) 742-6888
DAYTON, OHIO	(513) 226-0241
DENVER, COLORADO	(303) 837-8638
DETROIT, MICH.	(313) 962-6906
FT. LAUDERDALE, FL.	(305) 462-1818
FT. WORTH, TEXAS	(817) 338-9004
HOUSTON, TEXAS	(713) 224-6098
INDIANAPOLIS, INDIANA	(317) 632-8739
KANSAS CITY, MO.	(816) 836-1810
LOS ANGELES, CALF.	(213) 488-1871
LUBBOCK, TEXAS	(806) 744-8879
MIDLAND/ODESS, TEXAS	(915) 561-5130
MILWAUKEE, WISCONSIN	(414) 933-7351
MINNEAPOLIS, MINN.	(612) 341-2835
NEWARK, NJ.	(201) 645-9040
NEW ORLEANS, LA.	(504) 566-8970
NEW YORK, NY.	(212) 397-1020
OKLAHOMA CITY, OK.(#1)	(405) 525-8963
OMAHA, NEBRASKA	(402) 422-0306
PHILADELPHIA, PA.	(215) 561-3199
PHOENIX, AZ.	(602) 249-0716
PITTSBURG, PA.	(412) 281-4905
ST. LOUIS, MO.	(314) 342-0280
SAN ANTONIO, TEXAS	(512) 226-8505
SAN DIEGO, CALF.	(714) 560-1465
SAN FRANCISCO, CALF.	(415) 495-2500
SOUTH BEND, IND.	(219) 232-8036
STAMFORD, CT.	(203) 348-0929
TOLEDO, OHIO	(419) 243-2048
TUCSON, ARIZONA	(602) 622-0212
TULSA, OKLAHOMA	(918) 583-9082
WASHINGTON, D.C.	(202) 872-1847

Following are MCI Mail local access phone numbers:

Atlanta, GA.....	(404) 577-7363
Baltimore, MD.....	(301) 583-6850
Boston, MA.....	(617) 262-6468
Buffalo, NY.....	(716) 847-6050
Chicago, IL.....	(312) 856-9000
Cincinnati, OH.....	(513) 651-1204
Cleveland, OH.....	(216) 771-7177
Columbus, OH.....	(614) 221-3451
Dallas, TX.....	(214) 754-0461
Denver, CO.....	(303) 831-8139
Detroit, MI.....	(313) 962-5980
Ft. Worth, TX.....	(817) 338-4159
Hartford, CT.....	(203) 728-1909
Houston, TX.....	(713) 850-1005
Indianapolis, IN...	(317) 634-2208
Kansas City, MO....	(816) 474-3169
Long Island (Garden City Area), NY.	(516) 596-0404
Los Angeles, CA....	(213) 620-1449
Memphis, TN.....	(901) 523-9314
Milwaukee, WI.....	(414) 347-1769
Minneapolis, MN....	(612) 893-9462
Newark, NJ.....	(201) 623-0295
New York City, NY..	(212) 245-0355
Oakland, CA.....	(415) 540-1114
Philadelphia, Pa...	(215) 636-9060
Phoenix, AZ.....	(602) 266-1148
Pittsburgh, PA.....	(412) 261-9918
Rochester, NY.....	(716) 955-9850
Sacramento, CA.....	(916) 442-6986
San Diego, CA.....	(619) 268-1708
San Francisco, CA..	(415) 543-1560
San Jose, CA.....	(408) 995-6711
Santa Ana, CA.....	(714) 550-7128
Stamford, CT.....	(203) 325-8133
St. Louis, MO.....	(314) 991-1881
Washington, DC.....	(703) 525-6500

- National Toll-Free Access Number

----------(800) 323-0905----------

(800) 333-7751

See "Telephone Answering Service" pages in this directory.

Dial the One-Plus way. Saving money can be fun.

Every employee of the Telephone Company carries an identification card. We suggest that you refuse access to your premises to anyone who represents himself as from the telephone company, but who cannot so identify himself.

•You'll get faster service on your long distance calls by dialing the complete number, including "1" + Area Code whenever and wherever possible.

The best way to put an end to crank or prank calls is to hang up immediately. If it persists, however, call your service rep. at the tel. bus. ofc. Specially trained telephone people will work with law enforcement agencies to help solve the problem.

IF YOUR NUMBER
HAS BEEN CHANGED

...Advise friends of the change—they'll be able to call you more easily.

•Keep a smile in your voice.

•Be quick to answer your telephone calls. Be slow to hang up when making a call. Give the other fellow at least one minute to answer.

For Quick Reference!

You'll find names and numbers quickly and easily a second time, if you underline them in your directory when you first look them up. And you can get free personal directories to jot down your often called numbers by calling the tel. bus. ofc.

• For better service—speak directly into the telephone.

A volume control telephone is available through your telephone business office.

Keep a pad and pencil by the phone. It'll come in handy.

•Wait for dial tone.

✓
WHENEVER POSSIBLE
remain on the line after you've placed a call

Talk is cheap. . .When you call on Saturday.

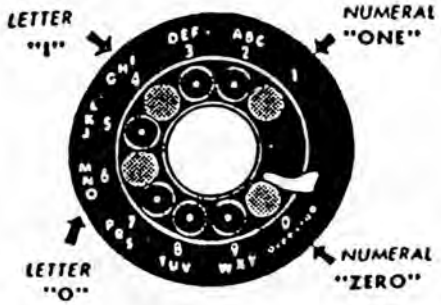
If you have any questions about your telephone bill, call your service representative at the business office.

False start?

If someone picks up an extension phone on your line while you're dialing, hang up and start again. The "click" from the extension pick-up may prevent the call from going through or may result in a wrong number.

please dial carefully

Please be careful not to confuse the letter "I" with the numeral "one," or the letter "O" with the numeral "zero" when dialing.



The following is a list of networks currently available on the Defense Data Network, including the base address of each. This is a complete, and up-to-date listing.

SATNET	4.0.0.0	YPG-NET-TEMP	6.0.0.0
EDN-TEMP	7.0.0.0	BBN-NET-TEMP	8.0.0.0
ARPANET	10.0.0.0	DODIIS	11.0.0.0
ATT	12.0.0.0	PDN	14.0.0.0
MIT	18.0.0.0	DDN-TC-NET	23.0.0.0
MINET	24.0.0.0	RSRE-EXP	25.0.0.0
MILNET	26.0.0.0	NOSC-LCCN-TEMP	27.0.0.0
WIDEBAND	28.0.0.0	UCL-TAC-NET	32.0.0.0
SU-NET-TEMP	36.0.0.0	SRI-LOCAL	39.0.0.0
BBN-TEST-A	41.0.0.0	AMPRNET	44.0.0.0
C3-PR	45.0.0.0	BERKELEY	46.0.0.0
SAC-PR-TEMP	47.0.0.0	BBN-TEST-B	128.1.0.0
CMU-NET	128.2.0.0	LBL-CSAM	128.3.0.0
DCNET	128.4.0.0	FORDNET	128.5.0.0
RUTGERS	128.6.0.0	DFVLR	128.7.0.0
UMDNET	128.8.0.0	ISI-NET	128.9.0.0
PURDUE-CS	128.10.0.0	BBN-CRONUS	128.11.0.0
SU-NET	128.12.0.0	MATNET	128.13.0.0
BBN-SAT-TEST	128.14.0.0	S1NET	128.15.0.0
UCLNET	128.16.0.0	MATNET-ALT	128.17.0.0
SRINET	128.18.0.0	EDN	128.19.0.0
BRLNET	128.20.0.0	SF-PR-1	128.21.0.0
SF-PR-2	128.22.0.0	BBN-PR	128.23.0.0
ROCKWELL-PR	128.24.0.0	BRAGG-PR	128.25.0.0
SAC-PR	128.26.0.0	DEMO-PR-1	128.27.0.0
C3-PR-TEMP	128.28.0.0	MITRE	128.29.0.0
MIT-NET	128.30.0.0	MIT-RES	128.31.0.0
UCB-ETHER	128.32.0.0	BBN-NET	128.33.0.0
NOSC-LCCN	128.34.0.0	CISLTESTNET1	128.35.0.0
YALE-NET	128.36.0.0	YPG-NET	128.37.0.0
NSWC-NET	128.38.0.0	NTANET	128.39.0.0
UCL-NET-A	128.40.0.0	UCL-NET-B	128.41.0.0
RICE-NET	128.42.0.0	CRANET	128.43.0.0
WSMR-NET	128.44.0.0	DODIIS-S1	128.45.0.0
DODIIS-S2	128.46.0.0	TACTNET	128.47.0.0
NOSC-ETHER	128.49.0.0	BBN-TEST-C	192.0.1.0
BBN-FIBRENET	192.1.2.0	BBN-JERICHO-NET	192.1.3.0
BBN-FIBER-TEST	192.1.4.0	BBN-ENET	192.1.7.0
BBN-STEAMER	192.1.128.0	CISLHYPERNET	192.5.1.0
WISC	192.5.2.0	HP-DESIGN-AIDS	192.5.3.0
HP-TCG-UNIX	192.5.4.0	DEC-MRNET	192.5.5.0
DEC-MRRAD	192.5.6.0	CIT-CS-NET	192.5.7.0
WASHINGTON	192.5.8.0	AERONET	192.5.9.0
ECLNET	192.5.10.0	CSS-RING	192.5.11.0
UTAH-NET	192.5.12.0	CCNET	192.5.13.0
RAND-NET	192.5.14.0	NYU-NET	192.5.15.0
LANLLAND	192.5.16.0	NRL-NET	192.5.17.0
IPTO-NET	192.5.18.0	UCIICS	192.5.19.0
CISLTTYNET	192.5.20.0	BRLNET1	192.5.21.0
BRLNET2	192.5.22.0	BRLNET3	192.5.23.0

BRLNET4	192.5.24.0	BRLNET5	192.5.25.0
NSRDCOA-NET	192.5.26.0	DTNSRDC-NET	192.5.27.0
RSRE-NULL	192.5.28.0	RSRE-ACC	192.5.29.0
RSRE-PR	192.5.30.0	CISLTESTNET2	192.5.32.0
CISLTESTNET3	192.5.33.0	CISLTESTNET4	192.5.34.0
RIACS-NET	192.5.35.0	CORNELL-CS	192.5.36.0
UR-CS-NET	192.5.37.0	SRI-C3ETHER	192.5.38.0
UDEL-EECIS	192.5.39.0	PUCC-NET-A	192.5.40.0
WISLAN	192.5.41.0	AFDSC-HYPER	192.5.42.0
CUCSNET	192.5.43.0	FARBER-PC-NET	192.5.44.0
AIDS-NET	192.5.45.0	NTA-RING	192.5.46.0
NSRDC	192.5.47.0	PURDUE-CS-IL	192.5.48.0
UCSF	192.5.49.0	CTH-CS-NET	192.5.50.0
THEORYNET	192.5.51.0	NLM-ETHER	192.5.52.0
UR-CS-ETHER	192.5.53.0	AERO-A6	192.5.54.0
UCLA-CECS	192.5.55.0	UDEL-CC	192.5.57.0
CSNET-PDN	192.5.58.0	AMES-NAS-NET	192.5.64.0
NPRDC-ETHER	192.5.65.0	HARV-NET	192.5.66.0
CECOM-ETHER	192.5.67.0	AERO-130	192.5.68.0
UIUC-NET	192.5.69.0	SCRC-ETHERNET	192.10.41.0

EASYLINK

CITY	BAUD RATE	CONNECT NUMBER
NEW YORK	110	212-608-7313
	300	212-608-7332
	1200	212-608-7480
PHILADELPHIA	110	215-592-4379
	300	215-592-4495
	1200	215-592-4377
DETROIT	110	313-962-4390
	300	313-962-4417
	1200	313-962-4393
CHICAGO	110	312-263-2314
	300	312-263-3723
	1200	312-263-2347
CINCINNATI	110	513-241-2488
	300	513-241-2819
	1200	513-241-2901
WASHINGTON DC	110	202-638-7694
	300	202-638-7579
	1200	202-638-7669
ST LOUIS	110	314-241-5440
	300	314-241-5601
	1200	314-241-6141
ATLANTA	110	404-659-3637
	300	404-659-3583
	1200	404-659-3606
HOUSTON	110	713-237-0361
	300	713-237-0431
	1200	713-237-1254
SAN FRANCISCO	110	415-989-6310
	300	415-989-6383
	1200	415-989-6300
LOS ANGELES	110	213-624-3213
	300	213-624-3227
	1200	213-624-4248

A PUBLIC SERVICE FOR E-COM SUBSCRIBERS WHO'VE LOST THEIR NUMBERS.

2028424458
2028424457
2028424427
2028424426
2028424428
2028424429
2066226870
2066227801
2065870139
2065870138
2065870135
2065870136
2125949064
2126951272
2126954577
2129473092
2125949068
2129472759
2136212634
2136212635
2136173541
2136173555
2136173628
2136173634
2147497947
2147497945
2147490757
2147490758
2146989154
2146989155
2153870184
2153870181
2153866002
2153866001
2153866003
2153866004
3038256793
3038256794
3035958433
3035958434
3035958435
3035958436
3058593591
3058593672
3058591399
3058591786
3058593427
3058593432

300/1200 ASYNC

2400/4800 BISYNC
(2780/3780 PROTOCOL)

3124610866
3124610867
3124610864
3124610865
3124610863
3124610869
3139652614
3139653783
3139653772
3139653773
3139653775
3139653776
3144365330
3144365340
3144363642
3144363671
3144363731
3144363742
4047630640
4047630664
4047611337
4047611376
4047611543
4047611620
4123913528
4123913153
4123913415
4123913416
4123913412
4123913414
4142726455
4142726500
4142715231
4142717691
4142713081
4142718592
4152821422
4152821421
4152822800
4152822801
4152822855
4152822856
5045233697
5045233724
5045246047
5045246073
5045247019
5045247242
5126535517 300
5126531935 1200
5126534938 2400
5126537940 2400
5126530007 4800
5126533041 4800

5134213804 300
5134213729 1200
5133815413 2400
5133815415 2400
5133815448 4800
5133816421 4800
6022538938 300
6022539683 1200
6022521827 2400
6022521828 2400
6022523775 4800
6022522776 4800
6123759089 300
6123759149 1200
6123330437 2400
6123330438 2400
6123330435 4800
6123330436 4800
6152422966 300
6152422970 1200
6152420849 2400
6152420856 2400
6152420870 4800
6152420875 4800
6175424301 300
6175424324 1200
6174516105 2400
6174516108 2400
6174516106 4800
6174516107 4800
7043939141 300
7043939142 1200
7043938245 2400
7043938276 2400
7043938304 4800
7043938325 4800
8043291536 300
8043291964 1200
8043291073 2400
8043291279 2400
8043291380 4800
8043291485 4800
8162212459 300
8162212537 1200
8162212940 2400
8162212673 2400
8162213077 4800
8162213115 4800

Jeanby/Süddeutsche Zeitung/Munich

New York Telephone

1095 Avenue of the Americas
New York, New York 10036

DATE. TODAY'S DATE

RE: PHONE NUMBER

YOUR NAME

YOUR STREET ADDRESS

YOUR CITY, STATE, ZIP

It is the Company's Policy to notify a subscriber when we receive a subpoena or summons for the subscriber's toll billing records.

However, if there is a certification for non-disclosure in the body of a criminal or legislative subpoena or summons or an accompanying letter referring thereto, signed by the individual who procured the issuance of the subpoena or summons, notification will be deferred for 90 days from the date of the subpoena or summons.

Accordingly, on DATE 90 DAYS AGO, we received a subpoena from WHOEVER'S BEHIND THIS WHOLE THING (US DEPT OF JUSTICE, ETC.) for the toll billing records for your telephone number. This subpoena contained a certification not to disclose for 90 days.

This Company, in response to this subpoena, furnished these toll records to NAME OF HEAD HONCHO on THE VERY SAME DATE 90 DAYS AGO.

The Company has no information as to the purpose of this request or the nature of the inquiry or investigation being undertaken. Any questions you may have should be referred to the above-mentioned agency.

Very truly yours,

J. F. Dwyer

Security Investigator.

THIS IS THE FAMOUS "LETTER OF DOOM" THAT SUSPECTED INDIVIDUALS GET FROM NEW YORK TELEPHONE WHEN THEIR LINES ARE BEING MONITORED BY VARIOUS LAW ENFORCEMENT AGENCIES. IN THIS CASE, IT'S OBVIOUS THAT THE PHONE COMPANY WOULD RATHER NOT BE INVOLVED, BUT LEGALLY THEY HAVE TO BE. IF, ON THE OTHER HAND, THE PHONE COMPANY ITSELF IS MONITORING YOUR LINES, ODDS ARE THAT YOU WON'T GET A LETTER AT ALL. SO IF YOU HAVEN'T RECEIVED ANY LETTERS LIKE THE ONE ABOVE, YOU SHOULD START WORRYING.

201	201-676-7070
202	202-384-9620
203	203-789-6815
204	204-949-0900
205	205-988-7000
206	206-382-8000
207	617-787-5300
208	303-293-2333
209	415-546-0118
212	518-471-8111
213	213-501-3255
214	214-698-9711
215	412-633-5600
216	614-464-2345
217	217-525-7000
218	402-345-0600
219	317-265-4834
301	301-534-1168
302	412-633-5600
303	303-293-2333
304	304-344-8041
305	912-784-0440
306	306-347-2878
307	303-293-2333
308	402-345-0600
309	217-525-7000
312	312-769-9600
313	313-223-8690
314	314-726-7142
315	518-471-8111
316	816-275-2782
317	317-265-4834
318	504-245-5330
319	402-345-0600
401	617-787-5300
402	402-345-0600
403	403-425-2652
404	912-784-0440
405	405-236-6121
406	303-293-2333
407	**********
408	415-543-6374
409	713-820-4112
412	412-633-5600
413	617-787-5300
414	608-252-6932
415	415-546-0107
416	416-922-6686
417	314-726-7142
418	514-287-5151
419	614-464-2345
501	405-236-6121
502	502-583-2861
503	503-241-3440
504	504-245-5330
505	303-293-2333
506	506-648-3041
507	402-345-0600
508	**********
509	206-382-8000
512	512-828-2501
513	614-464-2345
514	514-287-5151
515	402-345-0600
516	518-471-8111
517	313-232-8690
518	518-471-8111
519	416-922-6686
601	601-961-0877
602	303-293-2333
603	617-787-5300
604	*CLOSED 9/82
605	402-345-0600
606	502-583-2861
607	518-471-8111
608	414-252-6932
609	201-676-7070
612	402-345-0600
613	416-922-6686
614	614-464-2345
615	615-373-5791
616	313-223-8690
617	617-787-5300
618	217-525-7000
619	213-501-3255
701	402-345-0600
702	415-546-0118
703	804-747-1411
704	912-784-9111
705	416-922-6686
706	****N/A*****
707	415-546-0107
708	**********
709	****N/A*****
712	402-345-0600
713	713-820-4112
714	213-501-3255
715	608-252-6932
716	518-471-8111
717	412-633-5600
718	518-471-8111
719	**********
801	303-293-2333
802	617-787-5300
803	912-784-0440
804	304-344-8040
805	415-546-0118
806	512-828-2501
807	416-922-6686
808	212-334-4336
809	212-334-4336 (Bermuda Only)
812	317-265-4834
813	813-228-7871
814	412-633-5600
815	217-525-7000
816	816-275-2782
817	214-698-9711
818	213-501-3255
819	514-287-5151
901	615-373-5791
902	902-421-4110
903	****N/A*****
904	912-784-0440
905	****N/A*****
906	313-223-8690
907	****N/A*****
908	**********
909	**********
912	912-784-0440
913	816-275-2782
914	518-471-8111
915	512-828-2501
916	415-546-0118
917	**********
918	405-236-6121
919	912-784-0440

"We know who you are. We know what you want. We've got YOUR number."

200 ___ 201 ___ 202 ___ 203 ___ 204 ___ 205 ___ 206 ___ 207 ___ 208 ___ 209 ___
210 ___ 211 ___ 212 ___ 213 ___ 214 ___ 215 ___ 216 ___ 217 ___ 218 ___ 219 ___
220 ___ 221 ___ 222 ___ 223 ___ 224 ___ 225 ___ 226 ___ 227 ___ 228 ___ 229 ___
230 ___ 231 ___ 232 ___ 233 ___ 234 ___ 235 ___ 236 ___ 237 ___ 238 ___ 239 ___
240 ___ 241 ___ 242 ___ 243 ___ 244 ___ 245 ___ 246 ___ 247 ___ 248 ___ 249 ___
250 ___ 251 ___ 252 ___ 253 ___ 254 ___ 255 ___ 256 ___ 257 ___ 258 ___ 259 ___
260 ___ 261 ___ 262 ___ 263 ___ 264 ___ 265 ___ 266 ___ 267 ___ 268 ___ 269 ___
270 ___ 271 ___ 272 ___ 273 ___ 274 ___ 275 ___ 276 ___ 277 ___ 278 ___ 279 ___
280 ___ 281 ___ 282 ___ 283 ___ 284 ___ 285 ___ 286 ___ 287 ___ 288 ___ 289 ___
290 ___ 291 ___ 292 ___ 293 ___ 294 ___ 295 ___ 296 ___ 297 ___ 298 ___ 299 ___
300 ___ 301 ___ 302 ___ 303 ___ 304 ___ 305 ___ 306 ___ 307 ___ 308 ___ 309 ___
310 ___ 311 ___ 312 ___ 313 ___ 314 ___ 315 ___ 316 ___ 317 ___ 318 ___ 319 ___
320 ___ 321 ___ 322 ___ 323 ___ 324 ___ 325 ___ 326 ___ 327 ___ 328 ___ 329 ___
330 ___ 331 ___ 332 ___ 333 ___ 334 ___ 335 ___ 336 ___ 337 ___ 338 ___ 339 ___
340 ___ 341 ___ 342 ___ 343 ___ 344 ___ 345 ___ 346 ___ 347 ___ 348 ___ 349 ___
350 ___ 351 ___ 352 ___ 353 ___ 354 ___ 355 ___ 356 ___ 357 ___ 358 ___ 359 ___
360 ___ 361 ___ 362 ___ 363 ___ 364 ___ 365 ___ 366 ___ 367 ___ 368 ___ 369 ___
370 ___ 371 ___ 372 ___ 373 ___ 374 ___ 375 ___ 376 ___ 377 ___ 378 ___ 379 ___
380 ___ 381 ___ 382 ___ 383 ___ 384 ___ 385 ___ 386 ___ 387 ___ 388 ___ 389 ___
390 ___ 391 ___ 392 ___ 393 ___ 394 ___ 395 ___ 396 ___ 397 ___ 398 ___ 399 ___
400 ___ 401 ___ 402 ___ 403 ___ 404 ___ 405 ___ 406 ___ 407 ___ 408 ___ 409 ___
410 ___ 411 ___ 412 ___ 413 ___ 414 ___ 415 ___ 416 ___ 417 ___ 418 ___ 419 ___
420 ___ 421 ___ 422 ___ 423 ___ 424 ___ 425 ___ 426 ___ 427 ___ 428 ___ 429 ___
430 ___ 431 ___ 432 ___ 433 ___ 434 ___ 435 ___ 436 ___ 437 ___ 438 ___ 439 ___
440 ___ 441 ___ 442 ___ 443 ___ 444 ___ 445 ___ 446 ___ 447 ___ 448 ___ 449 ___
450 ___ 451 ___ 452 ___ 453 ___ 454 ___ 455 ___ 456 ___ 457 ___ 458 ___ 459 ___
460 ___ 461 ___ 462 ___ 463 ___ 464 ___ 465 ___ 466 ___ 467 ___ 468 ___ 469 ___
470 ___ 471 ___ 472 ___ 473 ___ 474 ___ 475 ___ 476 ___ 477 ___ 478 ___ 479 ___
480 ___ 481 ___ 482 ___ 483 ___ 484 ___ 485 ___ 486 ___ 487 ___ 488 ___ 489 ___
490 ___ 491 ___ 492 ___ 493 ___ 494 ___ 495 ___ 496 ___ 497 ___ 498 ___ 499 ___
500 ___ 501 ___ 502 ___ 503 ___ 504 ___ 505 ___ 506 ___ 507 ___ 508 ___ 509 ___
510 ___ 511 ___ 512 ___ 513 ___ 514 ___ 515 ___ 516 ___ 517 ___ 518 ___ 519 ___
520 ___ 521 ___ 522 ___ 523 ___ 524 ___ 525 ___ 526 ___ 527 ___ 528 ___ 529 ___
530 ___ 531 ___ 532 ___ 533 ___ 534 ___ 535 ___ 536 ___ 537 ___ 538 ___ 539 ___
540 ___ 541 ___ 542 ___ 543 ___ 544 ___ 545 ___ 546 ___ 547 ___ 548 ___ 549 ___
550 ___ 551 ___ 552 ___ 553 ___ 554 ___ 555 ___ 556 ___ 557 ___ 558 ___ 559 ___
560 ___ 561 ___ 562 ___ 563 ___ 564 ___ 565 ___ 566 ___ 567 ___ 568 ___ 569 ___
570 ___ 571 ___ 572 ___ 573 ___ 574 ___ 575 ___ 576 ___ 577 ___ 578 ___ 579 ___
580 ___ 581 ___ 582 ___ 583 ___ 584 ___ 585 ___ 586 ___ 587 ___ 588 ___ 589 ___
590 ___ 591 ___ 592 ___ 593 ___ 594 ___ 595 ___ 596 ___ 597 ___ 598 ___ 599 ___
600 ___ 601 ___ 602 ___ 603 ___ 604 ___ 605 ___ 606 ___ 607 ___ 608 ___ 609 ___
610 ___ 611 ___ 612 ___ 613 ___ 614 ___ 615 ___ 616 ___ 617 ___ 618 ___ 619 ___
620 ___ 621 ___ 622 ___ 623 ___ 624 ___ 625 ___ 626 ___ 627 ___ 628 ___ 629 ___
630 ___ 631 ___ 632 ___ 633 ___ 634 ___ 635 ___ 636 ___ 637 ___ 638 ___ 639 ___
640 ___ 641 ___ 642 ___ 643 ___ 644 ___ 645 ___ 646 ___ 647 ___ 648 ___ 649 ___
650 ___ 651 ___ 652 ___ 653 ___ 654 ___ 655 ___ 656 ___ 657 ___ 658 ___ 659 ___
660 ___ 661 ___ 662 ___ 663 ___ 664 ___ 665 ___ 666 ___ 667 ___ 668 ___ 669 ___
670 ___ 671 ___ 672 ___ 673 ___ 674 ___ 675 ___ 676 ___ 677 ___ 678 ___ 679 ___
680 ___ 681 ___ 682 ___ 683 ___ 684 ___ 685 ___ 686 ___ 687 ___ 688 ___ 689 ___
690 ___ 691 ___ 692 ___ 693 ___ 694 ___ 695 ___ 696 ___ 697 ___ 698 ___ 699 ___
700 ___ 701 ___ 702 ___ 703 ___ 704 ___ 705 ___ 706 ___ 707 ___ 708 ___ 709 ___
710 ___ 711 ___ 712 ___ 713 ___ 714 ___ 715 ___ 716 ___ 717 ___ 718 ___ 719 ___
720 ___ 721 ___ 722 ___ 723 ___ 724 ___ 725 ___ 726 ___ 727 ___ 728 ___ 729 ___
730 ___ 731 ___ 732 ___ 733 ___ 734 ___ 735 ___ 736 ___ 737 ___ 738 ___ 739 ___
740 ___ 741 ___ 742 ___ 743 ___ 744 ___ 745 ___ 746 ___ 747 ___ 748 ___ 749 ___
750 ___ 751 ___ 752 ___ 753 ___ 754 ___ 755 ___ 756 ___ 757 ___ 758 ___ 759 ___
760 ___ 761 ___ 762 ___ 763 ___ 764 ___ 765 ___ 766 ___ 767 ___ 768 ___ 769 ___
770 ___ 771 ___ 772 ___ 773 ___ 774 ___ 775 ___ 776 ___ 777 ___ 778 ___ 779 ___
780 ___ 781 ___ 782 ___ 783 ___ 784 ___ 785 ___ 786 ___ 787 ___ 788 ___ 789 ___
790 ___ 791 ___ 792 ___ 793 ___ 794 ___ 795 ___ 796 ___ 797 ___ 798 ___ 799 ___
800 ___ 801 ___ 802 ___ 803 ___ 804 ___ 805 ___ 806 ___ 807 ___ 808 ___ 809 ___
810 ___ 811 ___ 812 ___ 813 ___ 814 ___ 815 ___ 816 ___ 817 ___ 818 ___ 819 ___
820 ___ 821 ___ 822 ___ 823 ___ 824 ___ 825 ___ 826 ___ 827 ___ 828 ___ 829 ___
830 ___ 831 ___ 832 ___ 833 ___ 834 ___ 835 ___ 836 ___ 837 ___ 838 ___ 839 ___
840 ___ 841 ___ 842 ___ 843 ___ 844 ___ 845 ___ 846 ___ 847 ___ 848 ___ 849 ___
850 ___ 851 ___ 852 ___ 853 ___ 854 ___ 855 ___ 856 ___ 857 ___ 858 ___ 859 ___
860 ___ 861 ___ 862 ___ 863 ___ 864 ___ 865 ___ 866 ___ 867 ___ 868 ___ 869 ___
870 ___ 871 ___ 872 ___ 873 ___ 874 ___ 875 ___ 876 ___ 877 ___ 878 ___ 879 ___
880 ___ 881 ___ 882 ___ 883 ___ 884 ___ 885 ___ 886 ___ 887 ___ 888 ___ 889 ___
890 ___ 891 ___ 892 ___ 893 ___ 894 ___ 895 ___ 896 ___ 897 ___ 898 ___ 899 ___
900 ___ 901 ___ 902 ___ 903 ___ 904 ___ 905 ___ 906 ___ 907 ___ 908 ___ 909 ___
910 ___ 911 ___ 912 ___ 913 ___ 914 ___ 915 ___ 916 ___ 917 ___ 918 ___ 919 ___
920 ___ 921 ___ 922 ___ 923 ___ 924 ___ 925 ___ 926 ___ 927 ___ 928 ___ 929 ___
930 ___ 931 ___ 932 ___ 933 ___ 934 ___ 935 ___ 936 ___ 937 ___ 938 ___ 939 ___
940 ___ 941 ___ 942 ___ 943 ___ 944 ___ 945 ___ 946 ___ 947 ___ 948 ___ 949 ___
950 ___ 951 ___ 952 ___ 953 ___ 954 ___ 955 ___ 956 ___ 957 ___ 958 ___ 959 ___
960 ___ 961 ___ 962 ___ 963 ___ 964 ___ 965 ___ 966 ___ 967 ___ 968 ___ 969 ___
970 ___ 971 ___ 972 ___ 973 ___ 974 ___ 975 ___ 976 ___ 977 ___ 978 ___ 979 ___
980 ___ 981 ___ 982 ___ 983 ___ 984 ___ 985 ___ 986 ___ 987 ___ 988 ___ 989 ___
990 ___ 991 ___ 992 ___ 993 ___ 994 ___ 995 ___ 996 ___ 997 ___ 998 ___ 999 ___

The Hackers Guide to Area Code

C — Crossbar Office
E — Electronic or Digital Office
S — Step Office

A — AT&T
G — GTE
I — ITT
N — Northern Telecom

Date Completed _____

IBM 'ADS DIRECTORY'

DIV	ADS LOCATION	ADS TIELINE	ADS OUTSIDE
AFE	CANADA D MILLS	8/942/5261	416/443/5261
AFE	CANADA MARKHAM	8/241/2371	416/474/2371
AFE	CANADA MONTREAL	SEE (1)	514/874/4270
AFE	CANADA RTT1	SEE (2)	416/360/2721
AFE	CANADA RTT2	SEE (2)	416/360/5123
AFE	CANADA VANCOUVR	SEE (3)	604/665/8670
AFE	TARRYTOWN II	8/482/4333	914/997/4333
CHQ	ARMONK	8/251/5300	914/765/5300
CHQ	CCDN HCP	N/A YET	
CHQ	HUTCH CORP PARK	8/566/3300	914/684/3300
CPD	AUSTIN	8/678/8381	512/838/8381
CPD	AUSTIN	8/678/5555	512/838/5555
CPD	KINGSTON	8/373/1000	914/385/1000
CPD	RALEIGH	8/441/6801	919/543/6801
CSD	FRANKLIN LAKES	8/731/2200	201/848/2200
CSD	R 4 PHILADELPHA	8/943/2757	215/864/2757
DSD	POUGHKEEPSIE	N/A YET	
DSD	POUGHKEEPSIE	N/A YET	
EMEA	IBM EHQ	N/A YET	
EMEA	IBM FRANCE		331/296/1619
EMEA	IBM FRANCE	SEE (4)	
EMEA	IBM GERMANY	SEE (5)	
EMEA	IBM ITALY		39/275486550
EMEA	IBM UK		441/408/0787
EMEA	LA HULPE ED CTR	N/A YET	
FED	FRANKLIN LAKES	8/731/4545	201/848/4545
FED	GREENCASTLE	8/787/2020	317/658/2020
FSD	BETHESDA	8/765/1717	301/493/1717
FSD	GAITHERSBURG	8/372/6700	301/840/6700
FSD	HOUSTON	8/671/7788	713/333/7788
FSD	MANASSAS	8/725/5751	703/367/5751
FSD	OWEGO	8/662/5566	607/751/5566
FSD	OWEGO	8/662/5777	607/751/5777
GPD	SAN JOSE	N/A YET	
GPD	SAN JOSE	N/A YET	
GPD	SANTA THERESA	8/543/3055	408/463/3055
GPD	TUCSON	N/A YET	
ISCG	ISCGHQ W PLNS	8/524/4700	914/934/4700
ISG	FRANKLIN LAKES	8/731/4040	201/848/4040
ISG	ISGHQ KING ST	8/524/4700	914/934/4700
NAD	ATL REGION	8/728/4230	202/833/4230
NAD	DALLAS (GOSM)	8/668/1818	214/749/1818
NAD	DENVER B/O 13'	8/656/5222	303/773/5222
NAD	HOUSTON	8/345/1077	713/940/1077
NAD	INFO NTWK TAMPA	8/438/4300	813/872/4300
NAD	IRVING	8/641/5289	214/556/5289
NAD	LINE SW MKTG WP	8/367/4655	914/899/4655
NAD	NADHQ W PLNS	8/254/7100	914/696/7100
NAD	NFM BETHESDA	8/825/0311	301/493/0311
NAD	R 4 WAYNE, PA	8/432/5333	215/293/5333
NAD	R 6 ATLANTA	8/354/7550	404/885/7550
NAD	R 7 CINCINNATI	8/635/7610	513/733/7610
NAD	R 8 SOUTHFIELD	8/348/5555	313/552/5555
NAD	R 9 CHICAGO	8/261/4444	312/245/4444
NAD	R10 BLMTN, MN	8/653/2195	612/893/2195

NOTES:

(1) DIAL 8/241/2111 ASK FOR OUTSIDE NUMBER
(2) DIAL 8/241/2111 ASK FOR 8/165/4270
(3) DIAL 8/241/2111 ASK FOR 8/187/8670
(4) DIAL ADS 39-935-8400 EXT 4970
(5) DIAL ADS 49-7031-6200 EXT 6000

a directory

DIV	ADS LOCATION	ADS TIELINE	ADS OUTSIDE
NAD	R11 ST LOUIS	8/775/9473	314/554/9473
NAD	R13 S FRANCISCO	8/473/4747	415/545/4747
NAD	R14 L ANGELES	8/285/4400	213/736/4400
NAD	590 MADISON	8/243/5600	212/407/5600
NAD	590 MADISON	8/243/5125	212/407/5125
NAD	590 MADISON	8/243/5186	212/407/5186
NMD	ASC 5 DALLAS	8/668/6262	214/888/6262
NMD	ASC 6 L ANGELES	8/285/6441	213/736/6441
NMD	NMDHQ ATLANTA	8/331/5155	404/238/5155
NMD	NMSC ROCHESTER	8/456/7360	507/287/7360
NMD	R 1/2/3 NY	8/325/2741	212/239/2741
NMD	R 4/5 PHIL/BETH	8/943/6414	215/864/6414
NMD	R 5 BETHESDA	8/727/2522	301/987/2522
NMD	R 6 ATLANTA	8/354/4970	404/393/6970
NMD	R 6-8 SE'S	8/354/4820	404/393/6820
NMD	R 8 CINCINNATI	8/635/7634	513/733/7634
NMD	R 9 BLMFLD HILL	8/348/6564	313/540/6564
NMD	R10 RLG MEADOWS	8/788/6450	312/981/6450
NMD	R11 EDEN PRAIRI	8/653/2685	612/893/2685
NMD	R12 OVERLAND PK	8/344/7387	913/661/7387
NMD	R13 DALLAS	N/A YET	
NMD	R14 DENVER	8/656/5315	303/773/5315
NMD	R15 NEWPORT BCH	8/288/3233	714/752/3233
NMD	R16 S FRANCISCO	8/473/4900	415/545/4900
RECD	RECDHQ TARRTWN	N/A YET	
RECD	TARRYTOWN II	N/A YET	
RES	YORKTOWN	8/862/3701	914/945/3701
SPD	BOCA RATON	8/443/0361	305/998/0361
SPD	BOCA RATON	8/443/8500	305/998/8500
SPD	ROCHESTER	8/456/7400	507/287/7400
SPD	SPDHQ W PLNS	8/236/1812	914/686/1812
SSD	DAYTON	8/529/4755	201/329/4755
TCP	PRINCETON	8/538/8845	609/734/8845
WTC	EMEA W PLNS	8/236/2626	914/686/2626

MORE THAN MEETS THE EAR

New York Telephon

158 West Central Avenue
Spring Valley, New York 10977
Phone (914) 425-9950

June 27, 1984

We have made several unsuccessful attempts to reach you by telephone to discuss an important matter concerning your telephone service in the New City area.

Our records indicate that you are not subscribing to Touch Tone Service but you are using a push button phone. It will be necessary for you to contact us no later than July 3rd so that we may convert your service to Touch Tone at the approriate charges. If you fail to do so you will not be a ble to make outgoing calls from your push button set after July 8th due to our new call processing system; which went into effect on June 9th.

The new system is designed to handle more calls and process them faster. Also, it allows for sophisticated calling capabilities called Custom Calling Services. These services are "Call Waiting, Call Forwarding, Speed Calling, and Three Way Calling".

You may want to subscribe to these services when your convert to Touch Tone.

Please contact me befor July 3rd, so that I can make the necessary arrangements to connect you line to Touch Tone and avoid any interruption in your outgoing service.

Sincerely,

(Mrs.) M.J. Coyne
Representative

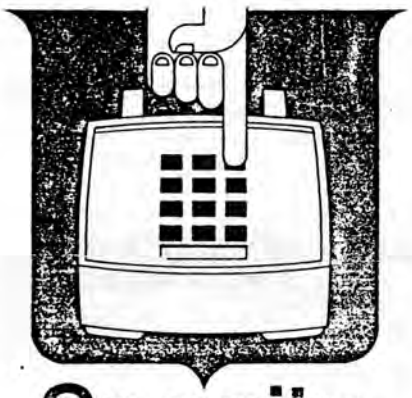
MC:ml

OH NO! THIS PERSON'S CENTRAL OFFICE HAS SWITCHED OVER TO ESS OR THE EQUIVALENT, WHICH MEANS NO MORE FREE USE OF TOUCH TONES®. AND SOMEHOW (PROBABLY THROUGH THE USE OF FCC REGISTRATION NUMBERS) THE PHONE COMPANY FOUND OUT THAT THIS PERSON WAS USING A "PUSH-BUTTON". BY THE WAY, CHECK OUT THE MANY TYPOS IN THIS LETTER. WE COUNTED FIVE MAJOR SCREWUPS, AND THERE ARE PROBABLY MORE.

BIOC

From the desk of 003

CONTACTING THE GESTAPO!



Security

as close as your fingertips

CORPORATE SECURITY

Director Corporate Security
~~J. E. Miller~~ 212-395-0505

SECURITY STAFF

Security Supervisor
W. F. McGarty 212-395-0528
Security Manager
R. F. Jobson 212-395-0552

NEW YORK CITY REGION

Security Manager
~~W. F. Breen~~ 212-395-4156

New York City West

Security Office 212-395-0515
Security Supervisor
J. R. Perk 212-395-0518

New York City East

Security Office 212-291-9617
Security Supervisor
C. J. Hauswirth 212-523-9953

STATE REGION

Suburban

Security Manager
J. J. Ferrari 914-699-9949

Mid-State

Security Office 914-699-9985
Security Supervisor
H. R. Zapf 914-699-9985

Long Island

Security Office 516-294-0210
Security Supervisor
R. H. Lamberson 516-294-0722

UPSTATE

Security Office 518-449-3250
Security Supervisor
T. A. Paolucci 518-449-5442
Security Manager
T. J. Doran 518-449-7224

TOLL FRAUD

Toll Fraud Office 212-221-1764
Security Supervisor
H. F. Gallagher 212-221-5844
Security Manager
J. S. Whitman 212-395-0507

On weekends, holidays and out of hours, call the following telephone numbers to obtain assistance.

Customer Service Bureau
New York City Region ... 212-395-2571
Mid-State 914-390-5600
Long Island 516-742-3030
Security Office
Upstate 518-449-3250

BUILDING PROTECTION ORGANIZATION

Guard Coordinators

New York City Region
W. J. Bluemel 212-394-3400*
State Region
H. K. Askildsen 914-694-8253*

**NOTE: These telephone numbers should be called concerning matters of building protection.*

C M German

J. J. Wells

New York Telephone

...GAR LANGUAGE
...m a different desk)

At the MCI Communications Corp. stockholders meeting in July a woman asked chairman William G. McGowan about a television spot featuring Joan Rivers. He explained that the ad brought in a lot of business although an operator from New Jersey Bell wrote him she was "really pissed off." The ad disparaged the long distance service of American Telephone and Telegraph Co. operators. While some in the hall seemed to think "pissed off" was vulgar, others didn't seem to notice. We asked MCI publicist Gary Tobin if anyone had complained. No one did, he said. "We are not the typical company. We are iconoclastic," Tobin added. "We are not like AT&T [in corporate culture]. The style is different." Because Tobin was so defensive we decided to check further.

According to the *Oxford English Dictionary*, piss is "not now in polite use". That 1973 dictionary suggested that at some time in the future the word might possibly make it into cultivated usage. Ten years later the *Dictionary of American Slang* listed the expression "pissed off" as taboo. But "the term passed into sophisticated use among the culturally elite and pseudo-elite," continued the lexicon.

Newspaper reporters are told not to quote the word "piss" but to bleep it out this way. "The governor said he was p— off."

President Lyndon Johnson once told an aide that the reason he kept his FBI director J. Edgar Hoover was that he was "now on the inside pissing out. If I fire him he would be on the outside pissing in."

"Pissed off" may be coming into more general use. It is one of several such terms for angry very widely used by the armed forces during World War II and carried into civilian life. The verb "piss" has been around a long time. It appears in Old English, Old French and the Old Testament and in Swift's *Elegy on Partridge*: "Whom roguish boys... Torment by pissing out their lights."

McGowan gets an excellent press. *Broadcasting* magazine published a profile on April 25, 1983, praising his business acumen.

In early 1983 MCI stock, one of the most actively traded on the OTC market, was bid as high as $46½. It sank to $6½ bid on July 26. The company is now much bigger than it was a few years ago, but access charges allowed AT&T by the FCC are pinching profits.

Bill McGowan speaks to stock analysts, women in telecommunications, congressional committees, conventions of various sorts. He has been called the world's greatest salesman. He claims he is speaking out more than any other executive of a billion dollar company. He has developed a style, a sense not only of what is correct language but also what will keep audiences of busy people from getting up and leaving him with empty chairs to talk to. He is constantly trying to talk up the MCI stock.

Did McGowan put his foot in his mouth or did he show his command of the colloquial idiom by using an expression most executives avoid in public? The word piss is one of "the seven dirty words" the Federal Communications Commission won't let you say on the radio or television. The FCC P.R. department will send you a press release on this, if asked. If the FCC's list of "dirty words" says the same, English keeps changing.

McGowan is an experimenter. "We say we don't know how to run this business. There is no role model to follow," McGowan told *Broadcasting*. "If we find a mistake, we'll change... You have to push to the outer edges. Business can be a terrible profession if done wrong. But a fantastic profession if done right, if it's pushed. If you enjoy doing things and accomplishing things and making things happen" and here he releases a rush of air between his teeth. "Woosh. the process is enjoyable."

MCI claims to have a telecommunications network second in size only to AT&T.

McGowan is a risk taker. He bought Western Union International and started MCI Mail. He sued AT&T and won. He tries out new things. He denied he is going to buy a computer company. Sometimes Wall Street agrees with what he does as in 1983 when MCI stock shot up. Now Wall Street isn't so sure about McGowan. Wall Street is pissed off at McGowan.

•Humm-mm-mm. That's the dial tone—your "go ahead" signal to start dialing. Please wait for it.

Answer Promptly

Don't make a friend wait or miss a call by not answering your telephone at once.

Area codes are used to call from one telephone area to another, but not within the same telephone area.

Dial-a-Discount. Dial-It-Yourself.

after you finish your call.....

be sure to replace the receiver

Try One-Plus Dialing.

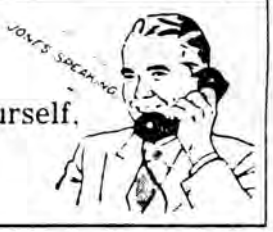
•Telephone cords and water don't mix. A wet cord can put your telephone out of order. So please keep your telephone cord away from sinks, valves, steam and other places where water might get on it.

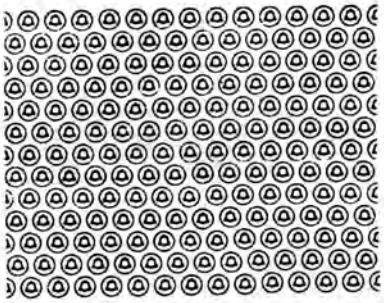
DIAL CAREFULLY!
Avoid wrong numbers by first checking the number and them
DIAL EACH DIGIT CAREFULLY!

The wheel that lets you roll around town without leaving home.

Just spin the dial and you're talking to the pharmacist. Spin it again and reach your insurance man. Or chat with a friend across town. Count on it any time — to save you time and traveling. Saves money, too. What else does so much yet costs so little?

WHEN ANSWERING THE TELEPHONE, always identify yourself, your firm, or your department.





when to get personal...

Station-to-station rates are always cheaper, so you should use person-to-person only when you want to talk to a particular party.

IF YOU'RE NEW IN TOWN...

shop the Yellow Pages

•Party-liners—don't forget the other fellow needs the telephone too.

•For better service, don't transfer a call to someone else if you can take care of it yourself.

when you're away from your office –*who'll answer your phone?*

See "Telephone Answering Service" pages in this directory.

NOT SURE OF THE NUMBER?

You'll save time and trouble if you look in the directory

Save time . . telephone.

When you're on the go . . . you're as close to home or office as the nearest public telephone booth . . . try it and see.

Alphabetical Listing of ICs and Carrier Identification Codes(CICs)

IC Name	ACNA	Old 2-Digit CIC	F.G. D 3-Digit CIC	F.G. B 3-Digit CIC
Allnet Communication Services, Inc.	ALN	44	444	044
ALTCOM Corporation	ALI	40	400	<--
Alternative Communications Company	ALT	34	234	<--
AmeriCall Systems of Louisville	ALU	06	006	<--
American Network, Inc.	PRH	53	053	<--
American Satellite Co.	ASC	56	369	<--
American Sharecom, Inc.	ASI	32	322	<--
American Telephone Exchange	ATE	50	050	<--
Argo Communications Corp.	ACC	45	456	<--
AT&T Communications	ATX	01	321	<--
Delta Communications, Inc.	DLT	30	233	<--
Eastern Telephone Systems, Inc.	ETS	54	054	<--
Express Telecom, Inc.	ETI	70	XXX	XXX
First Phone Corp.	FNE	42	442	<--
General Communication Inc.	GCN	77	077	<--
GTE SPRINT Communications	GSP	02	777	<--
HASP, Inc.	HAP	60	600	<--
Hawaiian Telephone Company	HWT	15	015	<--
Inteleplex Corporation	IPL	35	235	035
Interstate Communications, Inc.	ICI	87	087	<--
ISACOMM, Inc.	ISA	65	065	<--
Lehigh Valley Telcom, Inc.	LVT	51	051	<--
Lexitel Communications	LEX	66	666	066
Liberty Bell Communications, Inc.	LBC	76	776	<--
Long Distance Savers	LSI	36	036	<--
Long Distance Service (LDS), Inc.	LDS	84	084	<--
MCI International	MCX	13	???	<--
MCI Telecommunications Corporation	MCI	22	222	022
Mercury, Inc.	MEC	21	021	<--
Microtel, Inc.	MIC	78	789	<--
NCR Telecommunication Services Inc.	NCR	09	009	<--
Network I, Inc.	NEI	05	011	<--
Network Telecommunications	NTI	68	685	<--
Petricca Communications Systems	PEI	24	024	<--
RCI Corporation	RTC	03	211	003
Republic Telcom	RTT	26	026	<--
Satelco	SAN	80	800	<--
Satellite Business Systems	SBS	88	888	088
Schneider Communications	SCH	58	500	<--
Sears Communications Company	ALC	75	755	<--
Sorenson Telecommunications Company	STM	86	950	<--
Starnet Corporation	SNC	23	999	<--
TelaMarketing Communications, Inc.	TAM	07	007	<--
Telecom Systems, Inc.	TSS	89	889	<--
Telecommunications Systems, Inc.	TSI	52	852	<--
TeleDial America	TED	41	040	<--
Telesaver	TSR	28	221	<--

2-digit CIC is the XX portion of 950-10XX.
3 digit CIC (F.G. B) is the XXX portion of 950-1XXX.
3 digit CIC (F.G. D) is the XXX portion of 10XXX access code for areas that are equipped for equal access.
EXAMPLE: Inteleplex is currently reachable on 2-digit CIC at 950-1035. Under 3-digit CIC (F.G. B), they are still reachable at 950-1035. In areas equipped for equal access, the caller would simply dial 10235 to be connected to Inteleplex.

Alphabetical Listing of ICs and Carrier Identification Codes(CICs

IC Name	ACNA	Old 2-Digit CIC	F.G. D 3-Digit CIC	F.G. B 3-Digit CIC
Telesphere Network, Inc.	TEN	55	555	<--
Teltec Savings Communications Company	TET	31	031	<--
Total-Tel USA, Inc.	TTU	08	081	<--
Transcall America, Inc.	TRS	82	824	082
TRT Telecommunications Corporation	TRT	12	120	<--
U.S. Telephone, Inc.	UTC	33	333	033
United States Transmission Systems, Inc.	UST	25	488	<--
Universal Network Communications Co.	UVL	04	004	<--
WesTel, Inc.	WES	85	085	<--
Western Union Telegraph Company	WUT	20	220	<--

****
repared by: Numbering/Dialing Planning Group, Bellcore - Network Planning
or questions or comments call Bob Brillhart on 201-221-5315

MCI
Digital Information
Services Corporation
2000 M Street, NW
Suite 300
Washington, DC 20036
202 293 4255

MCI

BOY DO WE LOVE THESE PEOPLE

The folks at *2600* received this letter over a month ago. Naturally, we were intrigued by the idea of somebody publishing MCI Mail passwords! Had someone figured out a way to crack the system? We tried to reach this David Boyd fellow but were very unsuccessful. Instead we wound up talking to a surly individual who told us that he was unable to turn our account back on because he had no credit record on us. He asked us *all kinds* of questions and we seemed to convince him that we were legitimate. After 47 unreturned phone calls, he finally got back to us and said he was reactivating our account.

What's hard to understand here is why MCI Mail had to pull this crap about our password being published, when obviously nothing of the sort had occurred. We received many calls this month from "non-legitimate" subscribers who had gotten the very same letter. While we can see MCI Mail's concern about abused accounts (which was their own stupid fault; they made it so damn easy—see page 25), we can't understand why they tried to go after us—we weren't ripping them off at all. While it's impossible to get solid proof, all evidence points to the fact that they didn't like the *content* of the messages we were getting, meaning that they browse through their subscribers' mail, to make sure they're talking about the right things.

As of this printing, the account is still inactive. We're sorry about all the mail that is continuing to pile up in there, but there's nothing at all we can do. Perhaps a few complaints/threats are in order from our many customers.

Dear Customer:

It has been brought to our attention that your password and username have been published. Because unauthorized users could therefore charge usage to your account, we are temporarily inactivating it for your protection.

Please call us at 800-424-6677 to register for a new password and username. Any messages in your inactivated account will be available under your new account.

During registration, you will be asked to provide a credit card number (AMEX, VISA or Mastercard) and your SSN. These numbers will be used for credit check purposes only.

We regret any inconvenience this may have caused, but hope you will appreciate our concern for the protection of your MCI Mail account.

Sincerely,

David Boyd

David Boyd

SOME, BUT NOT ALL, ELECTRONIC MAIL SYSTEMS
WHICH MAY HAVE OTHER OPTIONS THAT WE DONT MENTION HERE

COMPANY NAME	SERVICE NAME	ON LINE PRICE*	DOWN LOAD PRICE**	800 INFO NUMBERS
ADP Autonet Ann Arbor, Mi	Automail	$48.63	$48.63	241-1945
Compuserve Corp Columbus, Ohio	Infoplex	$111.92	$111.92	428-2322
Computer Corp. of America Cambridge, Mass	Comet	$60.00	$60.00	222-2678
General Electric Information Services Corp. Rockville, Md	Quik-comm	$59.75	$51.00	638-8730
GTE Telenet Communications Corp. Vienna, Va	Telemail	$71.36	$31.34	354-2400
ITT Dialcom Silver Spring, Md	Dialcom	$70.76	$23.60	435-7342
MCI Communications Corp. Washington, D.C.	McMail	$102.50	$102.50	522-3222
Source Telecomputing Corp. McLean, Va.	Sourcemail	$110.23	$36.63	336-3366
Tymshare, Inc. Cupertino, Ca.	Ontyme	$58.76	$50.19	523-2263
Western Union Telegraph Co. Upper Saddle River, N.J.	EasyLink	$78.88	$34.89	325-6000

The above information is based on sending 35 msgs. (35,000 characters) to 93 recipients, and much of it is from ON COMMUNICATIONS.
* - Create msgs. on line ** - Download previously created msgs.

The following is a nifty list of voice messaging systems:

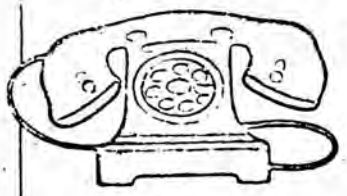
BBI Insustries Inc. - Voice Retrieval System
Centigram Corp. - Voice memo
Commterm Inc - EVX
Digital Sound Corp. - Voiceserver
Genesis Electronics Corp. - Cindi
IBM - Audio Distribution System
Octel Communications Corp. - Aspen
Rolm Corp. - Phonemail
Sudbury Systems Inc. - Voice Server
Voicemail International Inc. - Voice Mail System
VMX Inc. - Voice Message Exchange
Wang Laboratories Inc. - Digital Voice Exchange

We suggest that you investigate them and tell us what you find, but to get you started try Centigram at 800.321.6366

Reach Out and Goose Someone

Hours of pleasure from your telephone

by Paul D. Lehrman



Everybody knows about dial-a-prayer—in every city from Alaska to Australia you can assuage your god and your conscience without going any further than your phone. Many towns also have numbers you can call that will give you the latest sports scores or your daily horoscope. That stuff's easy to find. But there's a lot more entertainment available from your phone, and here's a list of some of those sources of entertainment, culled from the telephone directories of the English-speaking world:

ALTERNATIVE PRAYER

DIAL-AN-ATHEIST

~~Phoenix . . . . . (602)899-7411~~
Tucson . . . . . (602)623-3861
Washington, D.C. . . . . (202)370-5255
Los Angeles . . . . . (213)460-4326
Atlanta . . . . . (404)329-9809
Salt Lake City . . . . . (801)364-1939
Stoughton, Mass. . . . . (617)344-2988
Schenectady, N.Y. . . . . (518)346-1479
Charlotte, N.C. . . . . (704)568-5346
~~Milwaukee . . . . . (414)442-9786~~

DIAL-A-PRAYER IN SPANISH

Tucson . . . . . (602)296-3334

DIAL-A-SAINT

St. Louis . . . . . (314)421-4775

DIAL-A-MEDITATION

Boulder . . . . . (303)442-1471
Minneapolis . . . . . (612)861-7211
Seattle . . . . . (206)624-8985
New York City . . . . . (with Sri Chinmoy) (212)526-1111

DIAL-A-MIRACLE

Portland, Ore. . . . . (503)234-1443

DIAL-AN-ECK MESSAGE

Pittsburgh . . . . . (412)682-6432

DIAL-THE-BIBLE

Lynchburg, Va. . . . . (804)528-0401

DIAL-A-MOMENT-WITH-CHRIST

Ottawa, Ont. . . . . (613)820-8240

DIAL-A-TORAH-THOUGHT

Buffalo, N.Y. . . . . (716)832-2446

DIAL-A-SONG-OF-ZION

Vancouver, B.C. . . . . (604)876-9511

JOKES

(X means no one under 18 allowed to dial)

DIAL-A-SMILE

Santa Fe . . . . . (505)988-4000
Tulsa . . . . . (918)749-6611

DIAL AN' SMILE

Memphis . . . . . (901)278-2370

DIAL-A-SPAZZ

Marin County, Cal. . . . . (415)388-6633

BE FUNNY!

New York City . . . . . (212)338-5665

DIAL-A-CRAZY

Chicago . . . . . (312)528-4471

SMILE-A-PHONE WITH DR. DON (X)

San Francisco . . . . . (415)982-8778

KVPI JOKE LINE

Denver . . . . . (303)922-5653

THE MACHINE

Los Angeles . . . . . (213)833-3339

USE YOUR FINGER! (XXX)

Long Island, N.Y. . . . . (516)922-9463

STORIES

DIAL-A-STORY

Birmingham, Ala. . . . . (205)324-9911
Tucson . . . . . (602)326-1126
Little Rock, Ark. . . . . (501)661-1132
Louisville . . . . . (502)774-8409

INTERNATIONAL STORY LINE

Cambridge, Mass. . . . . (617)864-8819

POETRY

DIAL-A-VERSE

Miami . . . . . (305)443-6600

PHONE-A-POEM

Cambridge, Mass. . . . . (617)492-1144

MESSAGES THAT MAKE YOU FEEL BETTER

DIAL-A-SPIRITUAL-LIFT-UP

Denver . . . . . (781)2980

DIAL-A-LIFT-FOR-LIVING

Chicago . . . . . (312)332-6080

DIAL-FOR-COURAGE

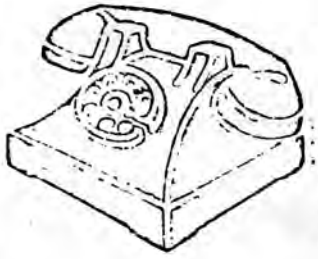
Portland, Ore. . . . . (503)224-1143

DIAL-AN-ANSWER

Denver . . . . . (303)443-2275

DIAL-A-CARE-THOUGHT

Denver . . . . . (303)321-7300



OUR FRIENDS, THE ANIMALS

DIAL-A-DOG

Sydney, Australia 389-8616

DIAL-A-BIRD

Schenectady, N.Y. . . . . (518)377-9600

DIAL-A-BOBCAT

Sydney, Australia 638-4476

VOICE OF AUDUBON

Lincoln, Mass. . . . . (617)259-8805

HEALTH, NUTRITION & BAD HABITS

DIAL-A-PUFF

Nashville . . . . . (615)329-9099
Memphis . . . . . (901)276-8003

DIAL-A-BOTTLE

Toronto . . . . . (416)447-1188

DIAL-A-HEARING-SCREENING-TEST

Long Island, N.Y. . . . . (516)369-1313
San Francisco . . . . . (415)776-1291

DIAL-YOUR-DOCTOR

Toronto . . . . . (416)492-4713

DIAL-NEW-TRITION

Washington, D.C. . . . . (202)986-9116

PHILOSOPHY & OBSERVATIONS

DIAL-A-THOUGHT

Detroit . . . . . (313)345-5070
St. Louis . . . . . (314)544-3311
San Francisco . . . . . (415)731-7710

DIAL-A-TAPE

Pittsburgh . . . . . (312)935-3333

DIAL-A-MESSAGE

Washington, D.C. . . . . (202)568-8580

DIAL-A-NEW-IDEA

Vancouver, B.C. . . . . (604)733-8914

FREEKYFONE

Woodland Hills, Cal. . . . (213)993-3466

THE ALTERNATIVE

Westminster, Cal. . . . . (714)891-1257

COMMERCE & SERVICES

DIAL-A-JOB

Memphis . . . . . (901)528-3434

DIAL-A-SERVICE

Toronto . . . . . (416)447-1188

DIAL-A-HOME-IMPROVEMENT

Toronto . . . . . (416)282-9770

RENTOKIL

Vistabella, Trinidad 652-2252

DIAL-DOW-JONES

New York City . . . . . (212)999-4141

MUSIC & PERFORMANCE

DIAL-A-SONG

Los Angeles . . . . . (213)664-7664

DIAL-A-CULTURAL-EVENT

St. Louis . . . . . (314)531-1111

PHONESONG

Cambridge, Mass. . . . . (617)491-0500

SOUNDSTAGE

Los Angeles . . . . . (213)666-7093

THANX

Hollywood . . . . . (213)769-8880

THIS IS 212-787-3231

New York City . . . . . (212)787-3231

BIZARRE STUFF

DIAL-A-PHENOMENON (SMITHSONIAN)

Washington, D.C. . . . . (202)357-2000

EARTH AND SPACE REPORT (HARVARD UNIV.)

Cambridge, Mass. . . . . (617)491-1497

Participatory numbers. These break down into two categories—party lines, which you dial into and talk to a bunch of folks simultaneously, and comment lines, where you dial in to hear what other folks have said, and then call the input number to record your own message, which will then be edited by the intrepid phone freaks who run the things, and played to the waiting world. Subjects range from the profound to the ridiculous.

PARTY LINES

DIAL-A-STRANGER

San Rafael, Cal. . . . . (415)461-7571

COMMENT LINES

DIAL-OGUE

Hartford, Conn. . . . . (203)232-3107

FEEDBACK

Sun Valley, Cal. . . . . (213)765-6000
Input . . . . . (213)765-5050

MONTAGE

Hollywood . . . . . (213)660-2000
Input . . . . . (213)660-2800

OBSERVATORY

Woodland Hills, Cal. . . . (213)999-0429
Input . . . . . (213)344-0110

SAN DIEGO COMMENT LINE

San Diego, Cal. . . . . (714)692-1000